bitdefender
internet security 2010

Manual de utilizare

BitDefender Internet Security 2010
Manual de utilizare

Publicat 2010.04.20

Termeni legali


bitdefender

Cuprins

Contract de licență pentru utilizatorul final

DACĂ NU SUNTEȚI DE ACORD CU ACEȘTI TERMENI ȘI CU ACESTE CONDIȚII NU INSTALAȚI ACEST SOFT. SELECTÂND "ACCEPT", "OK", "CONTINUĂ", "DA" SAU INSTALÂND SAU UTILIZÂND SOFTUL ÎN ORICE FEL INDICAȚI COMPLETA ÎNȚELEGERE ȘI ACCEPTARE A TERMENILOR CONTRACTULUI DE LICENȚĂ.

ÎNREGISTRARE PRODUS. Prin acordul exprimat față de conținutul acestui contract vă angajați să înregistrați produsul dvs., prin "Contul meu", aceasta reprezentând una dintre condițiile de utilizare ale produsului (pentru primirea actualizărilor) și de exercitare a dreptului la servicii de întreținere. Această măsură asigură folosirea produsului numai pe calculatoare cu licențe valabile și furnizarea de servicii de întreținere utilizatorilor finali deținători ai unor astfel de licențe. Înregistrarea presupune folosirea unei serii de înregistrare și a unei adrese de e-mail valabile, aceasta din urmă fiind necesară pentru reînnoirea licenței și pentru primirea altor notificări.

Acești Termeni acoperă soluțiile și serviciile BitDefender, incluzând documentația asociată și orice fel de actualizare a aplicației furnizată dumneavoastră în baza licenței achiziționate sau orice înțelegere de servicii asociată, definită în documentație, și orice copie a acestor obiecte.

Acest Contract de licență reprezintă o convenție legală între dumneavoastră (ca persoană fizică sau persoană juridică utilizator final) și BITDEFENDER pentru utilizarea produsului software identificat mai sus, aparținând BITDEFENDER, care include softul propriu-zis și serviciile, și poate include, medii de informație asociate, materiale tipărite și documentație "on line" sau electronică (referite în continuare ca "BitDefender"). Toate acestea sunt protejate de legislația internațională privind drepturile de autor și proprietatea intelectuală, precum și de tratatele internaționale. Prin instalarea, copierea sau utilizarea, în orice alt mod, a produsului BitDefender, acceptați termenii acestui contract.

Dacă nu sunteți de acord cu termenii acestui contract, nu instalați și nu utilizați produsul BitDefender.

Licența BitDefender. BitDefender este protejat de tratatele și legile internaționale privind drepturile de autor, precum și de celelalte legi și tratate privind proprietatea intelectuală BitDefender este oferit sub licență și nu vândut.

ACORDAREA LICENȚEI. BITDEFENDER vă oferă, dumneavoastră și numai dumneavoastră, următoarea licență ne-exclusivă, limitată, netransferabilă, cu titlu oneros, pentru utilizarea produsului BitDefender.

APLICAȚIA SOFTWARE. Puteți instala și utiliza BitDefender pe oricâte calculatoare este necesar în limita numărului total de licențe de utilizator deținute. Puteți face o singură copie adițională, ca rezervă.

LICENȚA UTILIZATORULUI DE DESKTOP. Această licență se aplică acelui soft BitDefender ce poate fi instalat doar pe un singur calculator și care nu furnizează servicii pentru rețele. Fiecare utilizator principal poate instala acest soft pe un singur calculator și poate face doar o singură copie adițională, ca rezervă, pe un dispozitiv diferit. Numărul de utilizatori principali permis este numărul de utilizatori ai licenței.

DURATA LICENȚEI. Licența acordată aici va începe la data la care veți instala BitDefender și va continua doar până la sfârșitul perioadei pentru care licența a fost achiziționată.

EXPIRARE. Produsul va înceta să mai funcționeze imediat după expirarea licenței.

ACTUALIZĂRI DE PRODUS (UPGRADE-URI). Dacă BitDefender este etichetat ca upgrade, va trebui să dețineți o licență de utilizare a unui produs identificat de BITDEFENDER ca fiind eligibil pentru respectivul upgrade. Un produs BitDefender etichetat ca fiind upgrade, înlocuiește și/sau completează produsul care reprezintă baza dreptului dumneavoastră de a beneficia de actualizarea de produs. Puteți utiliza produsul rezultat în urma actualizării numai în concordanță cu termenii specificați în prezentul Contract de Licență. Dacă BitDefender este un upgrade al unei componente a unui pachet de programe soft care v-au fost licențiate ca un singur produs, atunci BitDefender poate fi utilizat sau transferat numai ca parte a acelui pachet individual de produse și nu poate fi separat pentru utilizarea sa de către mai mulți utilizatori decât numărul de licențe. Termenii și condițiile acestei licențe înlocuiesc și prevalează orice alte înțelegeri care ar fi putut exista între dumneavoastră și BITDEFENDER privind produsul original sau produsul rezultat ca urmare a actualizării.

COPYRIGHT. Toate drepturile, titlurile și beneficiile ce țin de BitDefender (inclusiv, dar fără a se limita la orice imagine, fotografie, animație, video, audio, muzică, text și cod, încorporate în produsul BitDefender), toate materialele tipărite care însoțesc produsul și orice copie a produsului BitDefender sunt proprietatea BITDEFENDER. BitDefender este protejat de legile și tratatele internaționale privind drepturile de autor și proprietatea intelectuală. Prin urmare, BitDefender trebuie tratat ca orice alt material supus drepturilor de autor. Nu aveți dreptul să copiați materialele tipărite ce însoțesc BitDefender. Aveți obligația de a prezenta și include toate notele privind drepturile de autor în forma lor originală în toate copiile create, indiferent de mediul de transmisie sau de forma în care BitDefender există. Sunt interzise sub-licențierea, închirierea, vinderea, cedarea sau împărțirea licenței BitDefender. De asemenea, sunt interzise piratarea, recompilarea, dezasamblarea, crearea de produse derivate, modificarea, traducerea sau orice altă încercare de a descoperi codul sursă al produsului BitDefender.

LIMITAREA GARANȚIEI. BITDEFENDER garantează lipsa oricărui defect al suportului de distribuire al produsului BitDefender timp de 30 de zile de la data achiziționării acestuia. În cazul apariției unui defect al suportului de distribuire, ca unică modalitate de despăgubire pentru încălcarea acestei garanții, BITDEFENDER poate înlocui, la latitudinea sa, suportul defect returnat, cu un altul în schimbul chitanței sau vă

poate returna costul produsului BitDefender. BITDEFENDER nu garantează funcționarea neîntreruptă a produsului, lipsa erorilor sau posibilitatea corectării acestora. BITDEFENDER nu poate garanta ca produsele BitDefender corespund in totalitate cerințelor dumneavoastra.

CU EXCEPȚIA CELOR PRECIZATE ÎN MOD EXPLICIT ÎN ACEASTĂ ÎNȚELEGERE, BITDEFENDER ÎȘI DECLINĂ RESPONSABILITATEA PENTRU ORICE ALTE GARANȚII, EXPLICITE SAU IMPLICITE, CE PRIVESC PRODUSELE, ÎMBUNĂTĂȚIRILE, ÎNTREȚINEREA SAU SUPORTUL LEGAT DE ACESTEA, SAU ORICE ALTE MATERIALE (TANGIBILE SAU INTANGIBILE) SAU SERVICII FURNIZATE. BITDEFENDER DECLINĂ ÎN MOD EXPLICIT ORICE GARANȚII ȘI CONDIȚII IMPLICITE, INCLUZÂND, FĂRĂ LIMITARE, GARANȚIILE IMPLICITE ALE VANDABILITĂȚII, UTILIZĂRII ÎNTR-UN ANUMIT SCOP, TITLULUI, NON-INTERFERENȚEI, ACURATEȚEI DATELOR, A CONȚINUTULUI INFORMAȚIONAL, INTEGRĂRII SISTEMULUI ȘI NEÎNCĂLCĂRII DREPTURILOR UNOR TERȚE PĂRȚI PRIN FILTRAREA, DEZACTIVAREA SAU ÎNDEPĂRTAREA SOFTULUI ACESTORA, A APLICAȚIILOR SPYWARE, ADWARE, A FIȘIERELOR COOKIE, MESAJELOR E-MAIL, DOCUMENTELOR, RECLAMELOR SAU A ALTORA DE GENUL, INDIFERENT DACĂ ACEASTA REIESE DIN STATUT, LEGE, FUNCȚIONARE SAU COMERȚ.

DECLINAREA RESPONSABILITĂȚII ÎN CAZ DE DAUNE. Orice persoană care utilizează, testează sau evaluează BitDefender își asumă riscul legat de calitatea și performanța acestuia. BITDEFENDER nu va fi responsabilă, în niciun caz, pentru daune de orice natură, incluzând, fără limitare, daune directe sau indirecte, rezultate din utilizarea, performanța sau livrarea BitDefender, chiar dacă BITDEFENDER a fost informată de existența sau posibilitatea apariției acestora.

UNELE STATE INTERZIC LIMITAREA SAU DECLINAREA RESPONSABILITĂȚII ÎN CAZUL DAUNELOR INDIRECTE, DECI CELE MENȚIONATE MAI SUS S-AR PUTEA SĂ NU SE APLICE ÎN CAZUL DUMNEAVOASTRĂ.

RESPONSABILITATEA BITDEFENDER NU VA DEPĂȘI, ÎN NICIUN CAZ, PREȚUL DE ACHIZIȚIE AL PRODUSULUI BITDEFENDER. Declarațiile de limitare și declinare a responsabilității de mai sus se vor aplica indiferent dacă acceptați să folosiți, evaluați sau testați BitDefender.

ANUNȚ IMPORTANT PENTRU UTILIZATORI. ACEST SOFT POATE CONȚINE ERORI ȘI NU ESTE PROIECTAT SAU DESTINAT UTILIZĂRII ÎNTR-UN MEDIU CU GRAD MARE DE RISC ȘI CARE NECESITĂ O PERFORMANȚĂ SAU FUNCȚIONARE ÎN CONDIȚII DE SECURITATE ABSOLUTĂ. ACEST PRODUS NU ESTE DESTINAT UTILIZĂRII ÎN OPERAȚIUNI DIN DOMENIUL AVIAȚIEI, SECTORUL NUCLEAR SAU SISTEME DE COMUNICAȚII, SECTORUL ARMAMENTULUI, SISTEME DIRECTE SAU INDIRECTE DE MENȚINERE A VIEȚII, CONTROLUL TRAFICULUI AERIAN SAU ORICE ALTĂ APLICAȚIE SAU INSTALAȚIE ÎN CARE APARIȚIA UNEI ERORI AR PUTEA CAUZA MOARTEA SAU RĂNIREA GRAVĂ A UNOR PERSOANE SAU DAUNE ALE PROPRIETĂȚII.

ACORD PENTRU COMUNICAREA PRIN MIJLOACE ELECTRONICE. BitDefender poate avea obligația să vă trimită notificări oficiale și alte mesaje despre produs sau despre serviciile de întreținere cu plată ori despre modul în care sunt folosite

informațiile pe care ni le puneți la dispoziție ("Comunicări"). BitDefender va trimite Comunicări prin notificările din interiorul produsului sau prin e-mail, pe adresa de e-mail înregistrată a utilizatorului primar sau va posta aceste Comunicări pe siteul său. Exprimându-vă acordul în legătură cu conținutul acestui Contract acceptați să primiți Comunicări exclusiv prin aceste mijloace electronice, recunoașteți și dovediți capacitatea dvs. de a accesa Comunicările de pe Siteuri.

Actualizări. Acceptând acest Contract, recunoașteți și sunteți de acord că sistemul dumneavoastră va fi utilizat pentru recepționarea si transmiterea de actualizări prin intermediul unui protocol de tip peer-to-peer. Protocolul va fi folosit exclusiv pentru transmiterea și recepționarea de actualizări BitDefender pentru fișierele de semnături.

TEHNOLOGII DE COLECTARE A DATELOR- BitDefender vă informează că ar putea utiliza, în anumite programe sau produse, tehnologii de colectare a datelor pentru a centraliza informații tehnice (inclusiv fișierele suspecte), îmbunătăți produsele, furniza și adapta serviciile conexe și pentru a împiedica folosirea fără licență sau ilegală a produsului sau apariția daunelor rezultate din acțiunea aplicațiilor cu potențial periculos. Acceptați ca BitDefender să folosească acest tip de informații în cadrul serviciilor oferite în legătură cu produsul și pentru a preveni și a opri acțiunea programelor cu potențial periculos pe calculatorul dvs.

Acceptând acest Contract, recunoașteți și sunteți de acord că tehnologia de securitate utilizată poate scana traficul într-un mod impersonal pentru a detecta codurile malware și pentru a preveni daunele care pot fi provocate acestea.

Recunoașteți și acceptați faptul că BitDefender poate furniza actualizări sau elemente suplimentare ale produsului, care se descarcă automat pe calculatorul dvs.

Prin acceptarea acestui Contract, sunteți de acord să încărcați fișiere executabile pentru ca serverele BitDefender să le scaneze. De asemenea, pentru a contracta și folosi programul, este posibil ca BitDefender să vă solicite furnizarea anumitor date cu caracter personal. BitDefender vă informează că va trata datele dumneavoastră cu caracter personal în conformitate cu legislația aplicabilă în vigoare și cu Politica sa de confidențialitate.

COLECTAREA DATELOR. Accesarea site-ului de către utilizator și achiziționarea de produse și servicii, precum și utilizarea de instrumente sau conținut prin intermediul site-ului web presupun prelucrarea unor date cu caracter personal. Un obiectiv esențial pentru BitDefender este respectarea legislației care reglementează prelucrarea datelor cu caracter personal, serviciile societății informaționale și comerțului electronic. Uneori, pentru a accesa produse, servicii, conținut sau instrumente vi se poate solicita furnizarea anumitor detalii personale. BitDefender garantează păstrarea confidențialității acestor date, în conformitate cu legislația care reglementează protecția datelor cu caracter personal, serviciile societății informaționale și comerțului electronic.

BitDefender respectă legislația aplicabilă privind protecția datelor și a luat măsurile tehnice și administrative necesare garantării securității datelor cu caracter personal pe care le colectează.

Declarați că toate datele pe care le veți furniza vor fi adevărate și exacte și vă angajați să informați BitDefender despre orice modificare a acestora. Aveți dreptul să vă opuneți prelucrării oricăror date care nu sunt esențiale pentru punerea în aplicare a contractului și folosirii lor în alte scopuri decât menținerea relațiilor contractuale.

În cazul în care oferiți detalii despre o terță parte, BitDefender nu va fi răspunzătoare pentru respectarea principiilor de informare și de obținere a acordului. Prin urmare, dumneavoastră veți fi cel care garantează faptul că ați informat în prealabil și ați obținut acordul deținătorului datelor pentru comunicarea acestora.

BitDefender, afiliații și partenerii săi vor trimite informații de marketing prin e-mail sau alte mijloace electronice numai acelor utilizatori care și-au exprimat acordul expres pentru primirea comunicărilor despre produse sau servicii sau a buletinelor de știri BitDefender.

Politica de confidențialitate a BitDefender vă garantează dreptul de a accesa, rectifica, elimina și obiecta față de prelucrarea datelor prin notificarea BitDefender prin e-mail la: juridic@bitdefender.com .

GENERAL. Această înțelegere se află sub incidența legilor din România și a regulamentelor și tratatelor internaționale privind drepturile de autor și proprietatea intelectuală. Jurisdicția exclusivă și locația judecării oricărei dispute ce ar putea reieși din acești termeni de licență va fi cea a tribunalelor din Romania.

În eventualitatea invalidității oricărei porțiuni a acestei Înțelegeri, respectiva invaliditate nu va afecta validitatea celorlalte porțiuni ale acestei Înțelegeri.

BitDefender și simbolurile BitDefender sunt mărci înregistrate ale BITDEFENDER. Toate celelalte mărci înregistrate utilizate în produs sau în materialele asociate sunt proprietatea deținătorilor lor de drept.

Licența va fi anulată imediat, fără a fi anunțat, în cazul în care încălcați oricare dintre termenii sau condițiile ei. În urma anulării licenței nu veți fi îndreptățit la returnarea banilor de către BitDefender sau oricare dintre distribuitorii BitDefender. Termenii și condițiile privind confidențialitatea și restricțiile de utilizare vor rămâne în vigoare și după orice anulare a licenței.

BITDEFENDER poate revizui acești termeni în orice moment, iar termenii revizuiți se vor aplica în mod automat versiunilor software corespunzătoare, distribuite cu termenii revizuiți. Dacă oricare parte a acestor termeni este găsită nulă și neavenită, acest lucru nu va afecta validitatea restului termenilor, ce vor rămâne în vigoare.

În cazul controverselor sau inconsistențelor dintre traducerile acestor termeni în alte limbi, va prevala versiunea în limba engleză publicată de BITDEFENDER.

Adresa de contact a BITDEFENDER: Strada Preciziei, nr. 24, clădirea H2, parter, sector 6, București, România; telefon: 40-21-206.34.70 sau Fax: 40-21-264.17.99; adresă de e-mail: office@bitdefender.com.

Prefață

Acest manual se adresează tuturor utilizatorilor care au ales **BitDefender Internet Security 2010** ca soluție de securitate pentru calculatoarele personale. Informațiile incluse în acest manual sunt destinate nu numai utilizatorilor avansați, ci și oricărei persoane care poate lucra în sistemul Windows.

Acest manual conține descrierea BitDefender Internet Security 2010 și va ghidează în procesul de instalare și configurare a produsului. Manualul vă oferă informații despre modul de folosire, actualizare, testare și personalizare a produsului. Astfel, veți putea obține cele mai bune rezultate de pe urma folosirii BitDefender Internet Security 2010.

Vă dorim o lectură plăcută și utilă.

1. Convenții utilizate în manual

1.1. Convenții tipografice

Manualul conține diferite stiluri de text, pentru o lectură cât mai ușoară. Aspectul și semnificația acestora sunt prezentate în tabelul de mai jos.

Aspect	Descriere
`sample syntax`	Exemplele de sintaxă sunt tipărite cu caractere `monospațiate`.
http://www.bitdefender.ro	Linkurile URL indică locații externe, pe serverele http sau ftp.
sales@bitdefender.ro	Adresele de e-mail sunt inserate în text ca adrese de contact.
„Prefață” (p. xvii)	Acesta este un link intern, către o locație din document.
`filename`	Numele fișierelor și ale directoarelor sunt tipărite cu caractere `monospațiate`.
option	Toate opțiunile produsului sunt tipărite cu caractere **aldine**
`sample code listing`	Liniile de cod sunt tipărite cu caractere `monospațiate`.

1.2. Atenționări

Atenționările sunt note din text, marcate grafic, care oferă informații suplimentare legate de paragraful respectiv.

Notă

Nota nu este decât o scurtă observație. Deși pot fi omise, notele pot furniza informații importante, cum ar fi o caracteristică specifică sau un link către un subiect asemănător.

Important

Acest lucru necesită atenția dumneavoastră și nu este recomandat să-l ocoliți. De obicei, aici se furnizează informații importante, dar nu cruciale.

Avertisment

Este vorba de informații cruciale, cărora trebuie să le acordați o mare atenție. Dacă urmați indicațiile, nu se va întâmpla nimic rău. Este indicat să citiți și să înțelegeți despre ce este vorba, deoarece aici se descrie ceva extrem de riscant.

2. Structura manualului

Manualul conține mai multe părți ce acoperă subiectele majore. În plus, vă este oferit un vocabular pentru clarificarea înțelesului anumitor termeni tehnici.

Instalare și dezinstalare . Instrucțiuni, pas cu pas, pentru instalarea BitDefender pe un calculator personal. Pornind de la condițiile prealabile necesare, sunteți ghidat de-a lungul întregului proces de instalare. În cazul în care doriți să dezinstalați BitDefender vi se oferă o descriere a procedurii în cauză.

Introducere. Conține toate informațiile de care aveți nevoie pentru a începe să folosiți BitDefender. Va sunt prezentate interfață BitDefender, modalitățile de remediere a problemelor, de configurare a setărilor și de înregistrare a produsului dvs.

Modul Intermediar. Prezintă interfața BitDefender în Modul Intermediar.

Modul Expert. O prezentare detaliată a interfeței BitDefender în Modul Expert. Sunteți învățat cum să configurați și să utilizați toate modulele BitDefender astfel încât să vă protejați eficient calculatorul împotriva oricăror amenințări (aplicații malițioase, spam, hackeri, conținut inadecvat și altele).

Integrarea în Windows și în aplicațiile terților. Vă prezintă modalitatea de folosire a opțiunilor BitDefender în meniul contextual Windows și a barelor de instrumente integrate în programele terțe compatibile cu BitDefender.

Ghid de instrucțiuni. Cum să realizați cele mai importante sarcini cu BitDefender.

Remedierea problemelor și asistența. Unde să căutați și unde să cereți ajutor în cazul în care apar situații neprevăzute.

BitDefender Rescue CD. Descriere a BitDefender Rescue CD. Vă ajută să înțelegeți și să utilizați caracteristicile oferite de acest CD de boot.

Vocabular. Vocabularul încearcă să explice unii termeni tehnici sau neobișnuiți pe care îi veți găsi în paginele acestui document.

3. Comentarii

Vă invităm să ne ajutați să îmbunătățim acest manual. Am testat și verificat toate informațiile, în măsura posibilităților noastre. Vă rugăm să ne scrieți despre orice inexactități pe care le veți găsi în această carte sau despre cum credeți că ar putea fi îmbunătățită, pentru a ne ajuta să vă oferim cea mai bună documentație.

Aveți la dispoziție următoarea adresă de e-mail documentation@bitdefender.com.

Important

Vă rugăm să scrieți în engleză sau română mailurile către adresa de mai sus pentru a le putea procesa cât mai eficient.

Instalare și dezinstalare

1. Cerințe de sistem

Puteți instala BitDefender Internet Security 2010 doar pe calculatoare pe care rulează următoarele sisteme de operare:

- Windows XP (32/64 biți) cu Service Pack 2 sau mai recent
- Windows Vista (32/64 biți) sau Windows Vista cu Service Pack 1 sau mai recent
- Windows 7 (32/64 biți)

Înainte de instalare, asigurați-vă că sistemul dumneavoastră îndeplinește cerințele hardware și software minime.

Notă

Pentru a afla sistemul de operare Windows care rulează pe calculatorul dumneavoastră, precum și informații hardware, faceți clic-dreapta pe iconița **My Computer** de pe desktop și apoi selectați **Properties** din meniu.

1.1. Cerințe de sistem minime

- 450 MB de spațiu liber pe hard disc
- Procesor de 800 MHz
- Memorie RAM:
  - 512 MB pentru Windows XP
  - 1 GB pentru Windows Vista și Windows 7
- Internet Explorer 6.0
- .NET Framework 1.1 (disponibil și în kitul de instalare)

1.2. Cerințe de sistem recomandate

- 600 MB de spațiu liber pe hard disc
- Intel Core Duo (1.66 GHz) sau procesor echivalent
- Memorie RAM:
  - 1 GB pentru Windows XP și Windows 7
  - 1,5 GB pentru Windows Vista
- Internet Explorer 7 (sau mai recent)
- .NET Framework 1.1 (disponibil și în kitul de instalare)

1.3. Aplicații în care se poate integra BitDefender

Protecția antiphishing este oferită doar pentru:

- Internet Explorer 6.0 sau mai recent
- Mozilla Firefox 2.5
- Yahoo Messenger 8.5
- Windows Live Messenger 8

Criptarea mesageriei instant (IM) este oferită doar pentru:

- Yahoo Messenger 8.5
- Windows Live Messenger 8

Protecția antispam este oferită pentru toți clienții de mail POP3/SMTP. Bara de comenzi antispam însă este integrată doar în:

- Microsoft Outlook 2000 / 2003 / 2007
- Microsoft Outlook Express
- Microsoft Windows Mail
- Thunderbird 2.0.0.17

2. Pregătirea pentru instalare

Pentru a instala BitDefender Internet Security 2010 fără probleme, parcurgeți acești pași prealabili:

- Asigurați-vă că sistemul pe care doriți să instalați BitDefender întrunește cerințele minime. În cazul în care calculatorul nu întrunește toate cerințele minime de sistem, BitDefender nu va fi instalat sau nu va funcționa în mod corespunzător, determinând reducerea vitezei de funcționare și instabilitatea sistemului. Pentru o listă completă a cerințelor de sistem, vă rugăm să accesați *„Cerințe de sistem”* (p. 2).
- Autentificați-vă pe calculator cu datele unui cont de administrator.
- Dezinstalați orice alt program de securitate de pe calculator. Rularea simultană a două programe de securitate poate afecta funcționarea lor și poate provoca probleme majore ale sistemului. Windows Defender va fi dezactivat implicit, înainte de inițierea instalării.
- Dezactivați sau dezinstalați orice alt program firewall de pe calculator. Rularea simultană a două programe firewall poate afecta funcționarea lor și poate provoca probleme majore ale sistemului. Windows Firewall va fi dezactivat implicit, înainte de inițierea instalării.

3. Instalarea BitDefender

Puteți instala BitDefender de pe CD-ul de instalare BitDefender sau folosind fișierul de instalare descărcat pe calculatorul dumneavoastră de pe site-ul BitDefender sau de pe alte site-uri autorizate (de exemplu, site-ul unui partener BitDefender sau un magazin online). Puteți descărca fișierul de instalare de pe site-ul BitDefender: http://www.bitdefender.ro/site/Downloads/.

- Pentru a instala BitDefender de pe CD, introduceți CD-ul în unitate. În câteva momente se va afișa un ecran de întâmpinare. Urmați instrucțiunile pentru a începe instalarea.

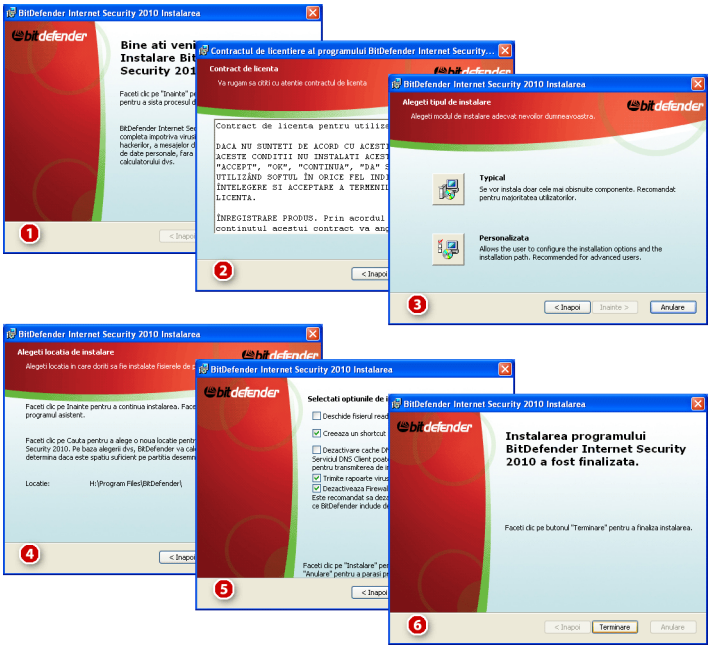
  Notă

  Ecranul de bun venit oferă o opțiune pentru copierea pachetului de instalare de pe CD-ul de instalare pe un dispozitiv de stocare USB. Acest lucru este util atunci când doriți să instalați BitDefender pe un computer care nu are o unitate CD (de exemplu, pe un netbook). Introduceți dispozitivul de stocare în unitatea USB și apoi faceți clic pe **Copiere pe USB**. Apoi, mergeți la calculatorul fără unitate de CD, introduceți dispozitivul de stocare în USB și faceți dublu-clic pe `runsetup.exe` din directorul în care ați salvat pachetul de instalare.

  Dacă ecranul de întâmpinare nu apare, urmați această cale: `Products\InternetSecurity\install\en\` din directorul rădăcină al CD-ului și faceți dublu-clic pe `runsetup.exe`.

- Pentru a instala BitDefender folosind fișierul de instalare descărcat pe calculator, localizați fișierul și faceți dublu-clic pe el.

Programul de instalare va verifica mai întâi sistemul dvs, pentru a valida instalarea. Dacă instalarea este validată, va apărea asistentul de instalare. În imaginea următoare sunt prezentați pașii programului asistent.



Etapele instalării

Urmați acești pași pentru a instala BitDefender Internet Security 2010:

1. Faceți clic pe **Înainte**. Puteți anula instalarea oricând doriți, făcând clic pe **Anulare**.

   BitDefender Internet Security 2010 vă alertează dacă aveți alte produse antivirus instalate pe calculatorul dumneavoastră. Faceți clic pe **Șterge** pentru a dezinstala produsul corespunzător. Dacă doriți să continuați fără a dezinstala produsele detectate, faceți clic pe **Înainte**.

   Avertisment
   Este recomandat să dezinstalați produsele antivirus detectate înainte de a instala BitDefender. Rularea a două sau mai multor produse antivirus în același timp, pe același calculator, provoacă în general instabilitatea sistemului de operare.

2. Vă rugăm să citiți cu atenție Contractul de licență și să faceți clic pe **Accept**.

   Important
   Dacă nu sunteți de acord cu prevederile acestui contract faceți clic pe **Anulare**. Procesul de instalare va fi abandonat și veți părăsi programul asistent.

3. Selectați tipul de instalare.
   - **Tipică** - pentru a instala programul imediat, folosind opțiunile de instalare implicite. Dacă alegeți această opțiune, treceți la pasul 6.
   - **Personalizată** - pentru a configura chiar dvs setările de instalare și pentru a instala apoi programul. Această opțiune vă permite să modificați calea de instalare.
4. În mod implicit, BitDefender Internet Security 2010 va fi instalat în `C:\Program Files\BitDefender\BitDefender 2010`. Dacă doriți să schimbați calea de instalare, faceți clic pe butonul **Caută** și selectați directorul în care doriți să fie instalat BitDefender.

   Faceți clic pe **Înainte**.
5. Selectați opțiuni referitoare la procesul de instalare. Opțiunile recomandate sunt selectate implicit:
   - **Deschide fișierul readme** - pentru deschiderea fișierului readme la sfârșitul instalării.
   - **Creează scurtătură pe desktop** - pentru a crea pe desktop o scurtătură (shortcut) către BitDefender Internet Security 2010 la sfârșitul instalării.
   - **Dezactivează cache DNS** - Pentru a dezactiva cache-ul DNS (Domain Name System). Serviciul DNS Client poate fi folosit de aplicațiile periculoase pentru transmiterea de informații în rețea fără permisiunea dvs.
   - **Trimite rapoarte de viruși** - Pentru a trimite rapoarte de scanare antivirus la Laboratorul BitDefender pentru analiză. Rapoartele nu conțin date confidențiale, cum ar fi numele dumneavoastră sau adresa IP, și nu vor fi folosite în scopuri comerciale.
   - **Dezactivează Firewallul Windows** - pentru a dezactiva aplicația Windows Firewall.

     Important

     Vă recomandăm să dezactivați Windows Firewall deoarece BitDefender Internet Security 2010 include un firewall avansat. Rularea simultană a două aplicații firewall pe un calculator poate provoca probleme.

   - **Dezactivează Windows Defender** - pentru a dezactiva aplicația Windows Defender; această opțiune apare numai pe Windows Vista.

   Faceți clic pe **Instalează** pentru a începe instalarea programului. Dacă nu este deja instalat, BitDefender va instala mai întâi .NET Framework 1.1.
6. Așteptați până când instalarea este finalizată și apoi faceți clic pe **Terminare** . Vi se va cere să reporniți sistemul pentru a finaliza procesul de instalare. Faceți acest lucru cât mai curând posibil.

Important

După finalizarea instalării și repornirea calculatorului, vor apărea un program asistent de înregistrare și un program asistent de configurare. Urmați pașii acestor programe asistent pentru a înregistra și configura BitDefender Internet Security 2010 și pentru a crea un cont BitDefender.

Dacă ați acceptat setările de cale implicite, veți observa că în directorul `Program Files` apare subdirectorul `BitDefender`, conținând un alt subdirector, `BitDefender 2010`.

3.1. Asistentul de înregistrare

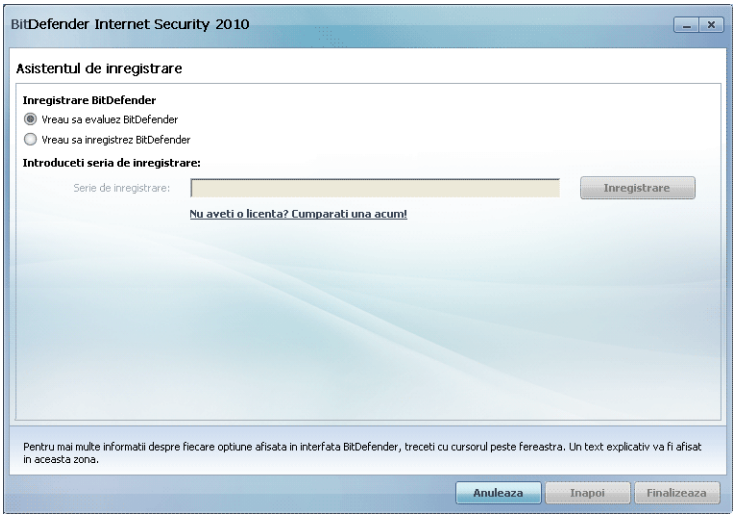
Prima dată când porniți calculatorul după instalare, va apărea un program asistent de înregistrare. Programul asistent vă ajută să înregistrați BitDefender și să configurați un cont BitDefender.

ESTE NECESAR să vă creați un cont BitDefender pentru a primi actualizări BitDefender. Contul BitDefender vă oferă acces la suport tehnic gratuit, oferte speciale și promoții. Daca v-ați pierdut seria de înregistrare BitDefender, puteți accesa contul dumneavoastră la http://myaccount.bitdefender.com pentru a o recupera.

Notă

Dacă nu doriți să urmați acest program asistent, faceți clic pe **Anulează**. Puteți deschide programul asistent de înregistrare oricând doriți, făcând clic pe linkul **Înregistrare**, situat în partea de jos a ferestrei principale a produsului.

3.1.1. Pasul 1 - Înregistrați BitDefender Internet Security 2010



Înregistrare

Perioada de evaluare a BitDefender Internet Security 2010 este de 30 de zile. Pentru a continua evaluarea produsului, selectați **Vreau să evaluez BitDefender** și faceți clic pe **Înainte**.

Pentru a înregistra BitDefender Internet Security 2010:

1. Selectați **Vreau să înregistrez BitDefender**.
2. Introduceți seria de înregistrare în câmpul editabil.

Notă

Puteți găsi seria dumneavoastră de înregistrare:

- pe eticheta de pe CD.
- pe certificatul de înregistrare al produsului.
- în e-mailul de achiziționare online.

Dacă nu aveți o serie de înregistrare BitDefender, faceți clic pe linkul furnizat pentru a merge la magazinul online BitDefender și a cumpăra una.

3. Faceți clic pe **Înregistrare**.
4. Faceți clic pe **Înainte**.

Dacă a fost detectată o serie de înregistrare BitDefender validă în sistemul dvs, o puteți folosi în continuare făcând clic pe **Înainte**.

3.1.2. Pasul 2 - Creați un cont BitDefender

Creare cont

Dacă nu doriți să creați un cont BitDefender în acest moment, selectați **Amână înregistrarea** si faceți clic pe **Finalizează**. Altfel, continuați în funcție de situația dumneavoastră actuală:

- „Nu am un cont BitDefender” (p. 10)
- „Deja am un cont BitDefender” (p. 11)

Important

Este necesar să vă creați un cont în termen de 15 zile de la instalarea BitDefender (dacă înregistrați produsul cu o serie de înregistrare, termenul limită se extinde la 30 de zile). În caz contrar, BitDefender nu se va mai actualiza.

Nu am un cont BitDefender

Pentru a crea un cont BitDefender, urmați acești pași:

1. Selectați **Creează cont nou**.
2. Introduceți informațiile solicitate în câmpurile corespunzătoare. Informațiile furnizate aici vor rămâne confidențiale.
   - **Adresă de e-mail** - introduceți adresa dvs. de e-mail.

- **Parolă** - introduceți o parolă pentru contul dumneavoastră BitDefender. Parola trebuie să conțină între 6 și 16 caractere.
- **Confirmați parola** - introduceți parola din nou.

Notă
După activarea contului, puteți folosi adresa de e-mail și parola furnizate pentru a-l accesa, la adresa http://myaccount.bitdefender.com.

3. Opțional, BitDefender vă poate informa despre oferte speciale și promoții folosind adresa de e-mail a contului dumneavoastră. Selectați una dintre opțiunile disponibile din meniu:
   - **Vreau sa primesc toate mesajele**
   - **Vreau sa primesc numai mesaje despre produs**
   - **Nu vreau sa primesc niciun mesaj**
4. Faceți clic pe **Creează**.
5. Faceți clic pe **Finalizează** pentru a încheia programul asistent.
6. **Activați-vă contul.** Pentru a vă putea utiliza contul, trebuie mai întâi să îl activați. Verificați-vă adresa de e-mail și urmați instrucțiunile din mesajul trimis de către serviciul de înregistrare BitDefender.

Deja am un cont BitDefender

BitDefender va detecta automat dacă ați creat anterior un cont BitDefender pe calculatorul dumneavoastră. În acest caz, furnizați parola contului dvs și faceți clic pe **Accesează**. Faceți clic pe **Finalizează** pentru a încheia programul asistent.

Dacă aveți deja un cont activ, dar BitDefender nu-l detectează, urmați pașii de mai jos pentru a înregistra produsul cu contul respectiv:

1. Selectați **Accesează cont creat anterior**.
2. Introduceți adresa de e-mail și parola contului dvs în câmpurile corespunzătoare.

Notă
Dacă v-ați uitat parola, faceți clic pe **V-ați uitat parola?** și urmați instrucțiunile.

3. Opțional, BitDefender vă poate informa despre oferte speciale și promoții folosind adresa de e-mail a contului dumneavoastră. Selectați una dintre opțiunile disponibile din meniu:
   - **Vreau sa primesc toate mesajele**
   - **Vreau sa primesc numai mesaje despre produs**
   - **Nu vreau sa primesc niciun mesaj**
4. Faceți clic pe **Accesează**.

5. Faceți clic pe **Finalizează** pentru a încheia programul asistent.

3.2. Asistentul de configurare

Odată ce ați finalizat programul asistent de înregistrare, va apărea un program asistent de configurare. Acest asistent vă permite să configurați principalele setări BitDefender și interfața cu utilizatorul, astfel încât acestea să corespundă mai bine cerințelor dumneavoastră. La sfârșitul programului asistent puteți să actualizați fișierele și semnăturile de viruși, precum și să scanați fișierele de sistem și aplicațiile pentru a vă asigura că nu sunt infectate.

Programul asistent constă în câțiva pași simpli. Numărul de pași depinde de alegerile pe care le faceți. Toți pașii sunt prezentați aici, dar veți fi anunțat când alegerile dvs influențează numărul acestora.

Nu este obligatoriu să urmați pașii programului asistent. Totuși, vă recomandăm să faceți acest lucru pentru a economisi timp și pentru a vă asigura că sistemul dumneavoastră nu era infectat înainte de a instala BitDefender Internet Security 2010. Dacă nu doriți să urmați acest program asistent, faceți clic pe **Anulează**. BitDefender vă va informa despre componentele care trebuie configurate atunci când deschideți fereastra principală a produsului.

3.2.1. Pasul 1 - Selectați profilul de utilizator

Profiluri de utilizator

Faceți clic pe butonul care descrie cel mai bine activitățile desfășurate pe acest calculator (profilul utilizatorului).

Opțiune	Descriere
Tipic	Faceți clic aici dacă acest calculator este folosit mai ales pentru navigare și activități multimedia.
Părinte	Faceți clic aici dacă acest calculator este folosit de copii și dacă doriți să controlați accesul acestora la Internet folosind modulul Control Parental.
Jucător	Faceți clic aici dacă acest calculator este folosit mai ales pentru jocuri.
Personalizat	Faceți clic aici dacă doriți să configurați toate setările principale ale BitDefender.

Puteți reseta profilul de utilizator ulterior, din interfața produsului.

3.2.2. Pasul 2 - Descrieți calculatorul

Descriere calculator

Selectați opțiunile care se aplică în cazul calculatorului dvs:

- **Acest calculator face parte dintr-o rețea personală.** Selectați această opțiune dacă doriți să administrați la distanță (de pe un alt calculator) produsul BitDefender instalat pe acest calculator. Un pas suplimentar al programului asistent vă permite să configurați modulul Administrare rețea personală.
- **Acest calculator este un laptop.** Selectați această opțiune dacă doriți ca Modul pentru laptop să fie activat în mod implicit. Dacă este activat Modul pentru laptop, sarcinile de scanare programate nu sunt efectuate atunci când laptopul se alimentează de la baterie deoarece acestea necesită mai multe resurse de sistem și sporesc, implicit, consumul de energie.

Faceți clic pe **Înainte** pentru a continua.

3.2.3. Pasul 3 - Selectați interfața

Moduri de vizualizarea a interfeței cu utilizatorul

Faceți clic pe butonul care descrie cel mai bine cunoștințele dvs de operare a calculatorului pentru a selecta modul corespunzător de vizualizare a interfeței cu utilizatorul. Puteți opta pentru vizualizarea interfeței cu utilizatorul în oricare dintre cele trei moduri, în funcție de cunoștințele dvs de operare a calculatorului și de gradul de familiarizare cu BitDefender.

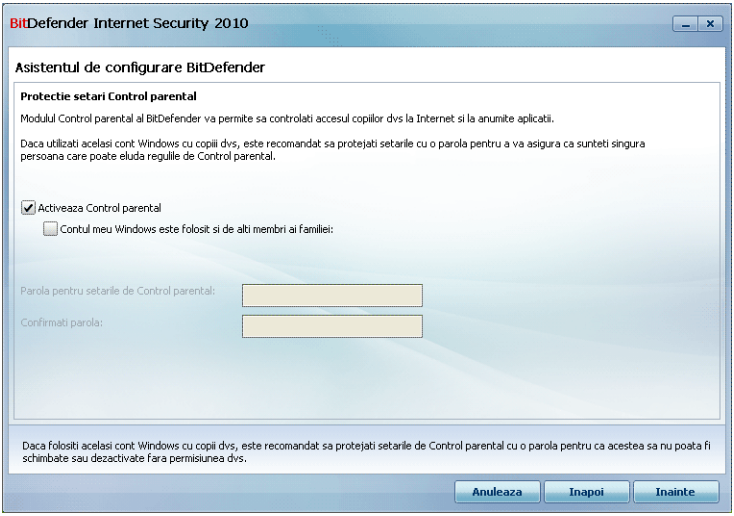
Mod	Descriere
Mod Novice	Potrivit pentru utilizatorii începători și pentru cei care doresc ca BitDefender să le protejeze calculatoarele și datele fără a fi solicitați să intervină. În acest mod, produsul este foarte ușor de utilizat, iar interacțiunea dvs cu el este minimă. Tot ce trebuie să faceți este să remediați problemele existente, atunci când sunt semnalate de BitDefender. Un program asistent intuitiv vă ghidează, pas cu pas, în acest proces. În plus, puteți efectua sarcini obișnuite, cum ar fi actualizarea semnăturilor de viruși din baza de date BitDefender și a fișierelor de produs, precum și scanarea calculatorului.

Mod	Descriere
Mod Intermediar	Destinat utilizatorilor cu abilități medii de folosire a calculatorului, acest mod extinde capacitățile de acțiune oferite în Modul novice. Puteți remedia problemele separat și puteți alege care dintre acestea să fie monitorizate. În plus, puteți administra la distanță produsele BitDefender instalate pe calculatoarele din rețeaua personală.
Mod Expert	Potrivit pentru utilizatori mai experimentați, acest mod vă permite să configurați complet fiecare funcționalitate BitDefender. De asemenea, puteți folosi toate sarcinile disponibile pentru a vă proteja calculatorul și datele.

3.2.4. Pasul 4 - Configurați controlul parental

Notă

Acest pas apare numai dacă ați selectat opțiunea **Personalizat** la Pasul 1.



Configurare Control parental

Controlul parental BitDefender vă permite să controlați accesul la Internet și la anumite aplicații pentru fiecare utilizator care deține un cont de utilizator pe sistem.

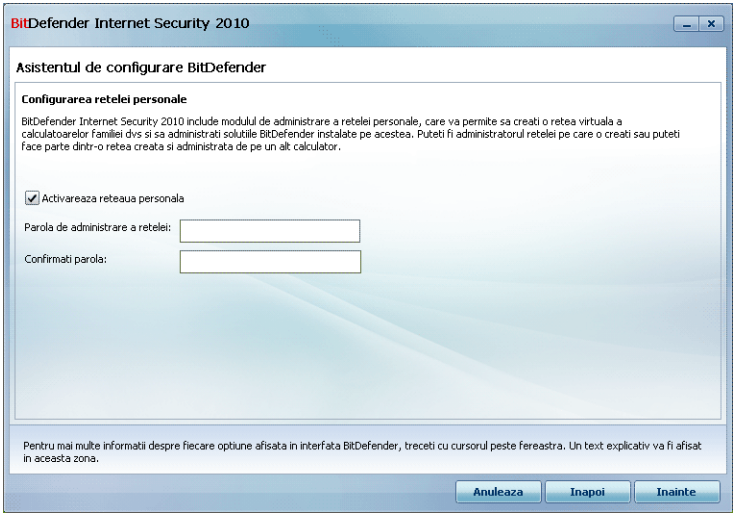
Dacă doriți să utilizați Controlul parental, urmați acești pași:

1. Selectați **Activează Control parental**.
2. Dacă folosiți același cont Windows cu copiii dvs, selectați căsuța corespunzătoare și introduceți o parolă, în câmpul respectiv, pentru a proteja setările de Control Parental. Oricine va încerca să schimbe setările de control parental, trebuie mai întâi să furnizeze parola pe care ați configurat-o.

Faceți clic pe **Înainte** pentru a continua.

3.2.5. Pasul 5 - Configurați rețeaua BitDefender

Notă
Acest pas apare numai dacă ați precizat, la Pasul 2, că acest calculator este conectat la o rețea personală.



Configurarea rețelei BitDefender

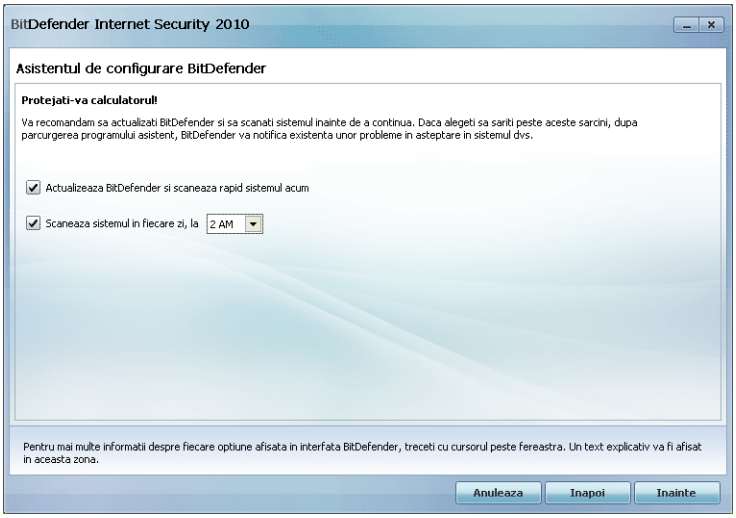
BitDefender vă permite să creați o rețea virtuală a calculatoarelor din locuința dumneavoastră și să administrați produsele BitDefender instalate în această rețea.

Dacă doriți ca acest calculator să fie parte a rețelei BitDefender, urmați acești pași:

1. Selectați **Activează rețeaua personală**.
2. Introduceți aceeași parolă administrativă în fiecare dintre câmpurile editabile. Parola permite unui administrator să administreze acest produs BitDefender de la un alt calculator.

Faceți clic pe **Înainte** pentru a continua.

3.2.6. Pasul 6 - Selectați sarcinile ce vor fi rulate



Selectare sarcini

Configurați BitDefender să execute sarcini importante privind securitatea sistemului dumneavoastră. Următoarele opțiuni sunt disponibile:

- **Actualizează BitDefender și scanează rapid sistemul acum** - la pasul următor, semnăturile de viruși și fișierele de produs ale BitDefender vor fi actualizate pentru protejarea calculatorului dvs împotriva celor mai noi amenințări. De asemenea, imediat după finalizarea actualizării, BitDefender va scana fișierele din directoarele `Windows` și `Program Files` pentru a verifica dacă acestea sunt infectate. Aceste directoare conțin fișierele sistemului de operare și ale aplicațiilor instalate și ele sunt, de obicei, primele infectate.
- **Scanează sistemul în fiecare zi la 2 AM** - setează BitDefender să efectueze o scanare standard a calculatorului dvs, în fiecare zi, la 2 AM. Pentru a schimba ora la care este efectuată scanarea, faceți clic pe meniu și selectați ora de începere dorită. Dacă aveți calculatorul închis atunci când sarcina trebuie să ruleze, aceasta va fi executată imediat ce deschideți calculatorul.

Notă

Dacă, mai târziu, doriți să modificați ora la care este programată să ruleze scanarea, urmați acești pași:

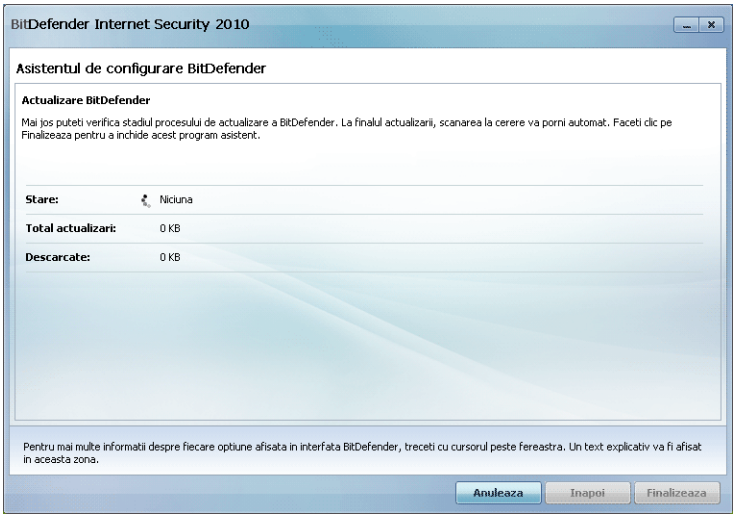
1. Deschideți BitDefender și treceți interfața în Modul Expert.

2. Faceți clic pe **Antivirus** în meniul din stânga.
3. Faceți clic pe tabul **Scanare viruși**.
4. Faceți clic-dreapta pe sarcina **Scanare de sistem** și selectați **Program**. Va apărea o nouă fereastră.
5. Modificați frecvența și momentul pornirii, după cum este necesar.
6. Faceți clic pe **OK** pentru a salva modificările.

Vă recomandăm să păstrați aceste opțiuni selectate înainte de a trece la pasul următor pentru a asigura securitatea sistemului dumneavoastră. Faceți clic pe **Înainte** pentru a continua.

Dacă deselectați prima căsuță, nu vor exista sarcini de efectuat la ultimul pas al programului asistent. Faceți clic pe **Finalizează** pentru a încheia programul asistent.

3.2.7. Pasul 7 - Finalizare



Stare sarcini

Așteptați ca BitDefender să-și actualizeze semnăturile de viruși și motoarele de scanare. Imediat ce actualizarea este finalizată, se va porni o scanare rapidă de sistem. Scanarea va fi efectuată discret, în fundal. Puteți observa iconița de scanare în curs în bara de sistem. Puteți face dublu-clic pe această iconiță pentru a deschide fereastra de scanare și a vedea evoluția scanării.

Faceți clic pe **Finalizează** pentru a încheia programul asistent. Nu este necesar să așteptați finalizarea scanării.

Notă

Scanarea va dura câteva minute. La finalul ei, deschideți fereastra de scanare și verificați rezultatele pentru a vedea dacă sistemul dumneavoastră este curat. Dacă au fost detectați viruși în timpul scanării, este recomandat să deschideți BitDefender imediat și să rulați o scanare completă a sistemului.

4. Actualizarea versiunii de produs

Puteți trece la o versiune superioară de produs, BitDefender Internet Security 2010, dacă folosiți BitDefender Internet Security 2010 beta sau versiunile 2008 ori 2009.

Există două moduri de trecere la o versiune superioară de produs:

- Instalarea BitDefender Internet Security 2010, direct peste versiunea mai veche. Dacă instalați direct peste versiunea 2009, Listele de prieteni și de spammeri, precum și Carantina vor fi importate în mod automat.
- Dezinstalați vechea versiune, apoi reporniți calculatorul și instalați noua versiune, conform instrucțiunilor de la capitolul *„Instalarea BitDefender”* (p. 5). Nicio setare de produs nu va fi salvată. Folosiți această metodă de trecere la o versiune superioară de produs dacă cealaltă nu funcționează.

5. Repararea sau dezinstalarea BitDefender

Dacă doriți să reparați sau să ștergeți BitDefender Internet Security 2010, urmați calea din meniul Start al Windows: **Start → Programe → BitDefender 2010 → Reparare sau dezinstalare**.

Vi se va solicita confirmarea alegerii prin apăsarea butonului **Înainte**. Va apărea o nouă fereastră, de unde puteți selecta:

- **Reparare** - pentru reinstalarea tuturor componentelor programului instalate anterior.

  Dacă alegeți să reparați BitDefender, va apărea o nouă fereastră. Faceți clic pe **Repară** pentru a iniția procesul de reparare.

  Reporniți calculatorul atunci când vi se va cere acest lucru și, după repornire, faceți clic pe **Instalare** pentru a reinstala BitDefender Internet Security 2010.

  După finalizarea procesului de instalare, va apărea o nouă fereastră. Faceți clic pe **Finalizare**.

- **Dezinstalare** - pentru dezinstalarea tuturor componentelor instalate.

  Notă
  Vă recomandăm să alegeți **Dezinstalare** pentru a asigura o reinstalare corectă.

  Dacă alegeți să dezinstalați BitDefender, va apărea o nouă fereastră.

  Important
  Dezinstalând BitDefender, nu veți mai fi protejat împotriva virușilor, a aplicațiilor spyware și a hackerilor. Dacă doriți activarea Windows Firewall și a Windows Defender (doar pe Windows Vista) după dezinstalarea BitDefender, selectați căsuțele corespunzătoare.

  Faceți clic pe **Dezinstalare** pentru a iniția ștergerea completă a BitDefender Internet Security 2010 de pe calculatorul dumneavoastră.

  După finalizarea procesului de dezinstalare, va apărea o nouă fereastră. Faceți clic pe **Finalizare**.

  Notă
  După ce procesul de dezinstalare este finalizat, vă recomandăm să ștergeți subdirectorul `BitDefender` din directorul `Program Files`.

Introducere

6. Descriere generală

O dată ce ați instalat BitDefender, calculatorul dumneavoastră este protejat. Dacă nu ați finalizat asistentul de configurare, trebuie să deschideți BitDefender cât mai curând posibil și să rezolvați problemele existente. Este posibil să fie nevoie să configurați anumite componente ale BitDefender sau să luați măsuri preventive pentru a vă proteja calculatorul și datele dumneavoastră. Dacă doriți, puteți configura BitDefender să nu vă avertizeze în legătură cu anumite probleme.

Dacă nu ați înregistrat produsul (inclusiv prin crearea unui cont BitDefender), amintiți-vă să faceți acest lucru până la încheierea perioadei de evaluare. Este necesar să vă creați un cont în termen de 15 zile de la instalarea BitDefender (dacă înregistrați produsul cu o serie de înregistrare, termenul limită se extinde la 30 de zile). În caz contrar, BitDefender nu se va mai actualiza. Pentru mai multe informații despre procesul de înregistrare, consultați secțiunea *„Înregistrare și Contul meu” (p. 52)*.

6.1. Deschiderea BitDefender

Pentru a accesa interfața principala a BitDefender Internet Security 2010, folosiți meniul Start al Windows, urmând calea **Start → Programe → BitDefender 2010 → BitDefender Internet Security 2010** sau, mai rapid, faceți dublu-clic pe iconița BitDefender din bara de sistem.

6.2. Moduri de vizualizarea a interfeței cu utilizatorul

BitDefender Internet Security 2010 îndeplinește deopotrivă cerințele persoanelor experimentate și pe cele ale începătorilor în utilizarea calculatorului. Interfața sa grafică este proiectată pentru a se potrivi fiecărei categorii de utilizatori.

Puteți opta pentru vizualizarea interfeței cu utilizatorul în oricare dintre cele trei moduri, în funcție de cunoștințele dvs de operare a calculatorului și de gradul de familiarizare cu BitDefender.

Mod	Descriere
Mod Novice	Potrivit pentru utilizatorii începători și pentru cei care doresc ca BitDefender să le protejeze calculatoarele și datele fără a fi solicitați să intervină. În acest mod, produsul este foarte ușor de utilizat, iar interacțiunea dvs cu el este minimă. Tot ce trebuie să faceți este să remediați problemele existente, atunci când sunt semnalate de BitDefender. Un program asistent intuitiv vă ghidează, pas cu pas, în acest proces. În plus, puteți efectua sarcini obișnuite,

Mod	Descriere
	cum ar fi actualizarea semnăturilor de viruși din baza de date BitDefender și a fișierelor de produs, precum și scanarea calculatorului.
Mod Intermediar	Destinat utilizatorilor cu abilități medii de folosire a calculatorului, acest mod extinde capacitățile de acțiune oferite în Modul novice. Puteți remedia problemele separat și puteți alege care dintre acestea să fie monitorizate. În plus, puteți administra la distanță produsele BitDefender instalate pe calculatoarele din rețeaua personală.
Mod Expert	Potrivit pentru utilizatori mai experimentați, acest mod vă permite să configurați complet fiecare funcționalitate BitDefender. De asemenea, puteți folosi toate sarcinile disponibile pentru a vă proteja calculatorul și datele.

Modul de vizualizare a interfeței cu utilizatorul se selectează în programul asistent pentru configurare. Acest program asistent apare după derularea celui de înregistrare, atunci când deschideți calculatorul prima dată după instalarea produsului. Dacă anulați programul asistent de configurare, interfața va fi afișata implicit în Modul intermediar.

Pentru a schimba modul de vizualizare a interfeței, parcurgeți următorii pași:

1. Deschideți BitDefender.
2. Faceți clic pe butonul **Setări** din colțul din dreapta, sus al ferestrei.
3. În categoria Setări interfață cu utilizatorul, faceți clic pe săgeata de pe buton și selectați modul dorit din meniu.
4. Faceți clic pe **OK** pentru a salva și aplica modificările.

6.2.1. Modul Novice

Dacă sunteți începător în operarea calculatorului, afișarea interfeței cu utilizatorul în Modul novice ar putea fi cea mai bună alegere pentru dvs. În acest mod, produsul este simplu de folosit și necesită o interacțiune minimă cu utilizatorul.

Modul Novice

Fereastra conține patru secțiuni principale:

- **Stare securitate** vă informează dacă sunt probleme care afectează securitatea calculatorului dumneavoastră și vă ajută să le rezolvați. Dacă faceți clic pe **Remediază**, un program asistent vă va permite să eliminați cu ușurință orice pericol la adresa calculatorului și a datelor dvs. Pentru mai multe detalii, consultați *„Remediere probleme”* (p. 40).
- **Protecție calculator** - aici puteți găsi sarcinile necesare pentru a vă proteja calculatorul și datele. Sarcinile disponibile pe care le puteți efectua diferă în funcție de profilul de utilizator selectat.
  - Butonul **Scanează acum** pornește o scanare standard a sistemului dvs, după viruși, programe spion și alte aplicații periculoase. Va apărea programul asistent Scanare antivirus, care vă va ghida în procesul de scanare. Pentru informații detaliate despre acest program asistent, consultați secțiunea *„Programul asistent de scanare”* (p. 57).
  - Butonul **Actualizează acum** vă permite să actualizați semnăturile de viruși și fișierele de produs ale BitDefender. Va apărea o nouă fereastră în care puteți vedea starea actualizării. Dacă sunt detectate actualizări, acestea sunt descărcate automat și instalate pe calculatorul dvs.
  - Când este selectat profilul **Tipic**, butonul **Caută vulnerabilități** pornește un program asistent care vă permite să identificați și să remediați vulnerabilitățile sistemului, cum ar fi: programe neactualizate și actualizări Windows lipsă.

Pentru informații detaliate, consultați secțiunea *„Asistent Verificare vulnerabilități”* (p. 69).

- Dacă este selectat profilul **Părinte**, butonul **Control parental** vă permite să configurați setările de Control parental. Controlul parental restricționează activitățile desfășurate pe calculator și online de către copii, pe baza regulilor definite de dvs. Restricțiile pot include blocarea accesului la site-uri web cu conținut inadecvat precum și limitarea accesului la jocuri și la Internet, în funcție de programul indicat. Pentru informații more referitoare la configurarea Controlului parental, consultați capitolul *„Control parental”* (p. 189).
- La selectarea profilului **Jucător**, butonul **Pornește/oprește Modul pentru jocuri** vă permite să activați/dezactivați Modul pentru jocuri. Modul pentru jocuri modifică temporar setările produsului pentru a minimiza impactul acestora asupra performanței sistemului.

- **Întreținere calculator** - aici puteți găsi sarcini suplimentare care vă permit să vă protejați calculatorul și datele.
  - **Adaugă fișier în seif** pornește programul asistent care vă permite să stocați în siguranță fișierele / documentele dumneavoastră importante criptându-le în partiții special, securizate (seife de fișiere).
  - **Scanare profundă de sistem** - pornește o scanare completă a sistemului dvs, după toate tipurile de programe periculoase.
  - **Scanare My Documents** - scanează după viruși și alte programe periculoase directoarele dvs cel mai des folosite: `My Documents` și `Desktop`. Astfel, documentele dvs sunt protejate, iar spațiul de lucru și aplicațiile care rulează la pornirea sistemului sunt sigure.
- **Profil utilizator** indică profilul de utilizator selectat. Profilul utilizatorului reflectă principalele activități desfășurate pe calculator. În funcție de profil, interfața produsului este organizată astfel încât să vă permită să accesați ușor sarcinile dvs favorite.

  Dacă doriți să treceți la un alt profil sau să-l editați pe care îl folosiți, faceți clic pe profil și urmați asistentul de configurare.

În colțul din dreapta, sus al ferestrei, se află butonul **Setări**. Acesta deschide o fereastră în care puteți schimba modul de vizualizare a interfeței cu utilizatorul sau dezactiva setările principale ale BitDefender. Pentru mai multe detalii, consultați *„Configurarea setărilor de bază”* (p. 44).

În colțul din dreapta, jos al ferestrei, puteți găsi mai multe link-uri utile.

Link	Descriere
Cumpără	Deschide o pagină web de unde puteți achiziționa o serie de înregistrare pentru produsul dumneavoastră BitDefender Internet Security 2010.
Înregistrare	Vă permite să introduceți o nouă serie de înregistrare sau să vedeți seria curentă de înregistrare și starea înregistrării.
Suport	Vă permite să contactați echipa de suport a BitDefender.
Ajutor	Deschide un fișier de ajutor care vă ajută să utilizați BitDefender.
Vizualizare jurnale	Vă permite să vedeți un istoric detaliat al tuturor sarcinilor efectuate de BitDefender pe sistemul dumneavoastră.

6.2.2. Modul Intermediar

Destinat utilizatorilor cu aptitudini medii de operare a calculatorului, Modul Intermediar afișează o interfață simplă, care vă oferă acces la toate modulele, la nivel de bază. În acest mod, va trebui să urmăriți avertismentele și alertele esențiale și să remediați problemele nedorite.

Modul Intermediar

Fereastra Mod intermediar conține cinci taburi. Tabelul de mai jos conține o scurtă descriere a fiecărui tab. Pentru mai multe detalii, consultați secțiunea „Modul Intermediar” (p. 95) a acestui manual.

Tab	Descriere
Stare	Afișează starea de securitate a sistemului dvs și vă permite să resetați profilul de utilizator.
Securitate	Afișează starea modulelor de securitate (antivirus, antiphishing, firewall, antispam, criptare mesagerie instant, confidențialitate, verificare vulnerabilități și actualizare) și linkuri către sarcini de verificare antivirus, actualizări și vulnerabilități.
Parental	Afișează starea modulului de control parental. Controlul parental vă permite să restricționați accesul copiilor la Internet și la anumite aplicații.
Seif pentru fișiere	Afișează starea seifului de fișiere și linkuri către seiful de fișiere.
Rețea	Afișează structura rețelei BitDefender. Aici puteți efectua diverse acțiuni pentru a configura și administra produsele BitDefender instalate în rețeaua dumneavoastră personală. În acest fel, puteți administra securitatea rețelei dumneavoastră personale de la un singur calculator.

În colțul din dreapta, sus al ferestrei, se află butonul **Setări**. Acesta deschide o fereastră în care puteți schimba modul de vizualizare a interfeței cu utilizatorul sau dezactiva setările principale ale BitDefender. Pentru mai multe detalii, consultați *„Configurarea setărilor de bază”* (p. 44).

În colțul din dreapta, jos al ferestrei, puteți găsi mai multe link-uri utile.

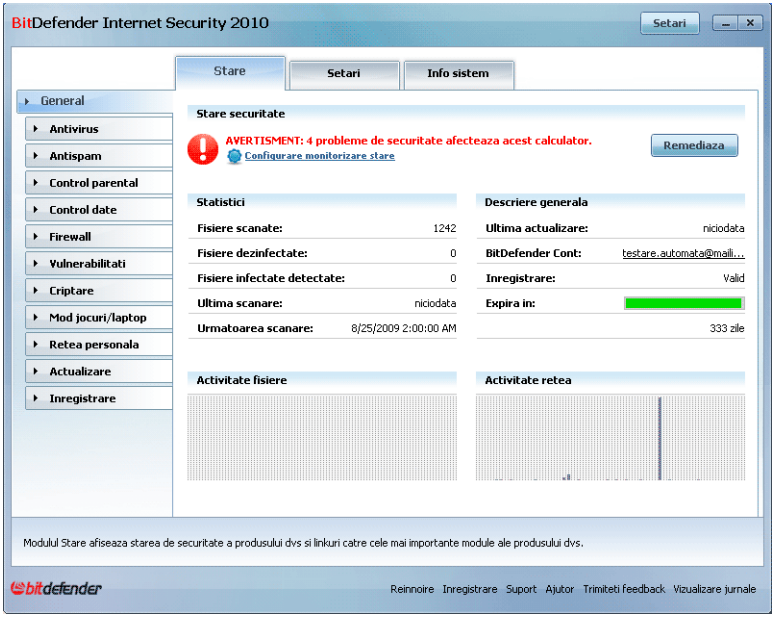
Link	Descriere
Cumpără	Deschide o pagină web de unde puteți achiziționa o serie de înregistrare pentru produsul dumneavoastră BitDefender Internet Security 2010.
Înregistrare	Vă permite să introduceți o nouă serie de înregistrare sau să vedeți seria curentă de înregistrare și starea înregistrării.
Suport	Vă permite să contactați echipa de suport a BitDefender.
Ajutor	Deschide un fișier de ajutor care vă ajută să utilizați BitDefender.

Link	Descriere
Vizualizare jurnale	Vă permite să vedeți un istoric detaliat al tuturor sarcinilor efectuate de BitDefender pe sistemul dumneavoastră.

6.2.3. Modul Expert

Modul Expert oferă acces la fiecare componenta a BitDefender. Aici puteți configura BitDefender în detaliu.

Notă
Modul Expert este potrivit pentru utilizatorii cu abilități de operare a calculatorului peste medie, care știu la ce fel de pericole este expus calculatorul și cum funcționează programele de securitate.



Modul Expert

În partea stângă a ferestrei există un meniu care conține toate modulele de securitate. Fiecare modul are unul sau mai multe taburi în care puteți configura setările de securitate corespunzătoare sau puteți efectua sarcini de securitate/administrative. Tabelul următor conține o scurtă descriere a fiecărui tab.

Pentru mai multe detalii, consultați secțiunea „Modul Expert” (p. 119) a acestui manual.

Modul	Descriere
General	Vă permite să accesați setările generale sau să vizualizați pagina de stare și informații detaliate despre sistem.
Antivirus	Vă permite să configurați scutul antivirus și operațiile de scanare în detaliu, să setați excepții și să configurați modulul de carantină.
Antispam	Vă permite să țineți la distanță mesajele spam de căsuța dumneavoastră de mesaje și să configurați setările antispam în detaliu.
Control parental	Vă permite să vă protejați copiii împotriva conținutului inadecvat utilizând regulile dumneavoastră privind accesul la calculator.
Control date	Vă permite să preveniți furtul de date de pe calculatorul dumneavoastră și să vă protejați confidențialitatea în timp ce sunteți online.
Firewall	Vă protejează calculatorul de tentative de conexiune neautorizată la ieșire sau la intrare. Modulul este asemănător unui paznic – supraveghează conexiunea la Internet și monitorizează aplicațiile cărora le este permis accesul la Internet precum și pe cele care trebuie blocate.
Vulnerabilitate	Vă permite să mențineți actualizate cele mai importante aplicații de pe calculatorul dumneavoastră.
Criptare	Vă permite să criptați comunicațiile prin Yahoo și Windows Live (MSN) Messenger și să criptați local fișierele, directoarele sau partițiile.
Mod jocuri/laptop	Vă permite să amânați executarea sarcinilor BitDefender programate cât timp laptopul dumneavoastră funcționează pe baterii și, de asemenea, să eliminați toate alertele și pop-upurile atunci când vă jucați pe calculator.
Rețea	Vă permite să configurați și să administrați mai multe calculatoare din locuința dumneavoastră.
Actualizare	Vă permite să obțineți informații despre cele mai recente actualizări, să actualizați produsul și să configurați procesul de actualizare în detaliu.

Modul	Descriere
Înregistrare	Vă permite să înregistrați BitDefender Internet Security 2010, să schimbați seria de înregistrare sau să creați un cont BitDefender.

În colțul din dreapta, sus al ferestrei, se află butonul **Setări**. Acesta deschide o fereastră în care puteți schimba modul de vizualizare a interfeței cu utilizatorul sau dezactiva setările principale ale BitDefender. Pentru mai multe detalii, consultați *„Configurarea setărilor de bază”* (p. 44).

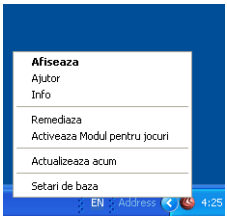
În colțul din dreapta, jos al ferestrei, puteți găsi mai multe link-uri utile.

Link	Descriere
Cumpără	Deschide o pagină web de unde puteți achiziționa o serie de înregistrare pentru produsul dumneavoastră BitDefender Internet Security 2010.
Înregistrare	Vă permite să introduceți o nouă serie de înregistrare sau să vedeți seria curentă de înregistrare și starea înregistrării.
Suport	Vă permite să contactați echipa de suport a BitDefender.
Ajutor	Deschide un fișier de ajutor care vă ajută să utilizați BitDefender.
Vizualizare jurnale	Vă permite să vedeți un istoric detaliat al tuturor sarcinilor efectuate de BitDefender pe sistemul dumneavoastră.

6.3. Iconiță în bara de sistem

Pentru a administra întregul produs mai rapid, puteți folosi iconița BitDefender din bara de sistem. Dacă faceți dublu-clic pe această iconiță, se va deschide fereastra BitDefender. De asemenea, făcând clic-dreapta pe iconiță, un meniu contextual vă va oferi posibilitatea unei administrări rapide a BitDefender.

- **Afișează** - deschide interfața principală a BitDefender.
- **Ajutor** - deschide documentația electronică, unde vi se explică în detaliu cum să configurați și să utilizați produsul BitDefender Internet Security 2010.
- **Despre** - deschide o fereastră în care puteți vedea informații despre BitDefender și unde să apelați pentru ajutor în cazul unei probleme.
- **Remediază** - vă ajută să remediați problemele curente de securitate. Dacă opțiunea nu este disponibilă, nu există



Iconiță în bară

probleme care trebuie remediate. Pentru mai multe detalii, consultați *„Remediere probleme”* (p. 40).

- **Activează/Dezactivează Modul pentru jocuri** - activează/dezactivează modul pentru jocuri.
- **Actualizează acum** - inițiază o actualizare imediată. Va apărea o nouă fereastră în care puteți vedea starea actualizării.
- **Setări de bază** - deschide o fereastră în care puteți schimba modul de vizualizare a interfeței cu utilizatorul și să activați sau să dezactivați setările principale ale produsului. Pentru mai multe informații, consultați secțiunea *„Configurarea setărilor de bază”* (p. 44).

Iconița BitDefender din bara de sistem vă informează despre problemele care vă afectează calculatorul sau despre funcționarea calculatorului, prin afișarea unui simbol special, după cum urmează:

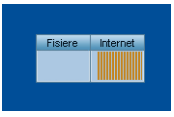
Triunghi roșu cu semnul exclamării: Probleme grave de securitate afectează calculatorul dvs. Acestea necesită atenția dvs imediat și trebuie remediate în cel mai scurt timp.
Litera G: Produsul funcționează în Modul pentru jocuri.

Dacă BitDefender nu funcționează, iconița din bara de sistem apare în gri. Acest lucru se întâmplă de obicei când expiră licența. O altă cauză poate fi faptul că serviciile BitDefender nu răspund sau că alte erori afectează funcționarea normală a produsului.

6.4. Bara de scanare

Bara de scanare este o reprezentare grafică a activității de scanare din sistemul dumneavoastră. Această fereastră mică este disponibilă, implicit, numai în Modul Expert.

Barele gri (zona **Fișiere**) reprezintă numărul de fișiere scanate pe secundă, pe o scară de la 0 la 50. Barele portocalii din zona **Internet** reprezintă numărul de kiloocteți transferați (trimiși și primiți de pe Internet) pe secundă, pe o scară de la 0 la 100.



Bara de scanare

Notă
Bara de scanare vă va avertiza când protecția în timp real sau protecția firewall este dezactivată prin afișarea unui X roșu deasupra zonei corespunzătoare (**Fișiere** sau **Internet**).

6.4.1. Scanare fișiere și directoare

Puteți utiliza bara de scanare pentru a scana rapid fișiere și directoare. Trageți fișierul sau directorul care doriți să fie scanat peste **Bara de scanare**, ca în imaginile de mai jos.

Trageți fișierul

Lăsați fișierul

Va apărea programul asistent Scanare antivirus, care vă va ghida în procesul de scanare. Pentru informații detaliate despre acest program asistent, consultați secțiunea *„Programul asistent de scanare”* (p. 57).

Opțiuni de scanare. Opțiunile de scanare sunt pre-configurate pentru a obține rata maximă de detecție. Dacă sunt detectate fișiere infectate, BitDefender va încerca să le dezinfecteze (va elimina codul malițios). Dacă dezinfectarea eșuează, programul asistent de scanare vă va permite să specificați alte acțiuni ce vor fi luate asupra fișierelor infectate. Opțiunile de scanare sunt standard și nu le puteți modifica.

6.4.2. Dezactivarea/Reactivarea barei de scanare

Când nu mai doriți să vedeți reprezentarea grafică, faceți doar clic-dreapta pe ea și selectați **Închide**. Pentru a reactiva bara de scanare, urmați acești pași:

1. Deschideți BitDefender.
2. Faceți clic pe butonul **Setări** din colțul din dreapta, sus al ferestrei.
3. În categoria Setări generale, selectați căsuța de lângă **Bara de scanare**.
4. Faceți clic pe **OK** pentru a salva și aplica modificările.

6.5. Scanare manuală BitDefender

Opțiunea Scanare manuală BitDefender vă permite să scanați un anumit director sau partiție de hard-disc, fără a crea o sarcină de scanare. Această funcționalitate a fost concepută pentru a fi utilizată atunci când Windows funcționează în Safe Mode. Dacă sistemul dumneavoastră este infectat cu un virus rezistent (care nu poate fi eliminat în urma unei scanări normale), puteți încerca să eliminați virusul pornind Windows în Safe Mode și scanând fiecare partiție de hard-disc folosind opțiunea Scanare manuală BitDefender.

Pentru a accesa programul asistent de scanare manuală, utilizați meniul Windows Start, urmând calea **Start → Programe → BitDefender 2010 → Scanare manuală BitDefender**. Va apărea următoarea fereastră:

Scanare manuală BitDefender

Faceți clic pe **Adaugă director**, locația care doriți să fie scanată și faceți clic pe **OK**. Dacă doriți să scanați mai multe directoare, repetați această acțiune pentru fiecare locație.

Căile către locațiile selectate vor apărea în coloana **Țintă scanare**. Dacă vă răzgândiți în legătură cu locația, faceți clic pe butonul **Șterge** de lângă aceasta. Faceți clic pe butonul **Elimină toate căile** pentru a elimina toate locațiile care au fost adăugate pe lista.

După ce ați terminat de selectat locațiile, faceți clic pe **Continuă**. Va apărea programul asistent Scanare antivirus, care vă va ghida în procesul de scanare. Pentru informații detaliate despre acest program asistent, consultați secțiunea *„Programul asistent de scanare”* (p. 57).

Opțiuni de scanare. Opțiunile de scanare sunt pre-configurate pentru a obține rata maximă de detecție. Dacă sunt detectate fișiere infectate, BitDefender va încerca să le dezinfecteze (va elimina codul malițios). Dacă dezinfectarea eșuează, programul asistent de scanare vă va permite să specificați alte acțiuni ce vor fi luate asupra fișierelor infectate. Opțiunile de scanare sunt standard și nu le puteți modifica.

Ce este Safe Mode?
Safe Mode este un mod special de a porni Windows, utilizat în principal pentru a depana problemele care afectează funcționarea normală a Windows. Aceste probleme variază de la conflicte provocate de drivere până la viruși care împiedică pornirea normală a Windows. În Safe Mode, Windows încarcă doar un minim de componente ale sistemului de operare și drivere de bază. Doar câteva aplicații funcționează în Safe Mode. Acesta este motivul pentru care majoritatea virușilor sunt inactivi și pot fi ușor eliminați atunci când Windows operează în Safe Mode.
Pentru a porni Windows în Safe Mode, reporniți calculatorul și apăsați tasta F8 încontinuu până apare meniul de opțiuni avansate al Windows (Windows Advanced Options Menu). Puteți alege între mai multe opțiuni de a porni Windows în Safe Mode. Este recomandat să selectați **Safe Mode with Networking** pentru a avea acces la Internet.

Notă

Pentru mai multe informații despre Safe Mode, consultați Centrul de Ajutor și Asistență al Windows (în meniul Start, faceți clic pe **Help and Support**). De asemenea, puteți găsi informații utile pe Internet.

6.6. Modul pentru jocuri și Modul pentru laptop

Unele activități efectuate pe calculator, cum ar fi jocurile sau prezentările, necesită o viteză sporită de reacție și funcționare a sistemului, fără întreruperi. Când laptopul dvs se alimentează de la baterie, este recomandat să amânați operațiile cu consum mare de energie până când laptopul este conectat din nou la o priză.

Pentru a se adapta la aceste situații, BitDefender Internet Security 2010 are două moduri de funcționare speciale:

- Modul pentru jocuri
- Modul pentru laptop

6.6.1. Modul pentru jocuri

Modul pentru jocuri modifică temporar setările produsului pentru a minimiza impactul acestora asupra performanței sistemului. Cât timp modul pentru jocuri este activat, se aplică următoarele setări:

- Se minimizează timpul de utilizare a procesorului și consumul de memorie.
- Se amână actualizările și scanările automate.
- Se elimină toate alertele și pop-upurile.
- Se scanează doar cele mai importante fișiere.

Cât timp modul pentru jocuri este activat, puteți vedea litera G pe  iconița BitDefender.

Utilizarea modului pentru jocuri

În mod implicit, BitDefender intră automat în modul pentru jocuri când porniți un joc din lista de jocuri cunoscute a BitDefender sau când o aplicație ocupă întreg ecranul (fullscreen). BitDefender va reveni automat la modul de funcționare normal atunci când închideți jocul sau când aplicația detectată iese din modul Ecran întreg.

Dacă doriți să activați modul pentru jocuri manual, folosiți una dintre următoarele metode:

- Faceți clic-dreapta pe icoana BitDefender din bara de sistem și selectați **Activează modul pentru jocuri**.
- Apăsați simultan tastele `Ctrl+Shift+Alt+G` (combinația de taste implicită).

Important
Nu uitați să dezactivați modul pentru jocuri atunci când ați încheiat jocul. În acest scop, utilizați aceleași metode ca și la activarea sa.

Schimbarea combinației de taste

Pentru a schimba combinația de taste, urmați acești pași:

1. Deschideți BitDefender și treceți interfața în Modul Expert.
2. Faceți clic pe **Mod jocuri/laptop** în meniul din stânga.
3. Faceți clic pe tabul **Mod jocuri**
4. Faceți clic pe butonul **Setări avansate**.
5. Sub opțiunea **Utilizează combinația de taste**, setați combinația de taste dorită:
   - Bifați tastele speciale pe care doriți să le folosiți: tasta Control (`Ctrl`), tasta Shift (`Shift`) sau tasta Alternate (`Alt`).
   - În câmpul editabil, tastați litera corespunzătoare tastei normale pe care doriți să o folosiți.

   De exemplu, dacă doriți să folosiți combinația de taste `Ctrl+Alt+D`, trebuie să bifați doar `Ctrl` și `Alt` și să tastați `D`.

   Notă
   Debifarea căsuței corespunzătoare opțiunii **Utilizați combinația de taste** va dezactiva combinația de taste.

6. Faceți clic pe **OK** pentru a salva modificările.

6.6.2. Modul pentru laptop

Modul pentru laptop este creat special pentru utilizatorii de laptopuri. Scopul acestuia este să minimizeze impactul pe care îl are BitDefender asupra consumului bateriei

atunci când aceste dispozitive funcționează pe baterie. Dacă este activat Modul pentru laptop, sarcinile de scanare programate nu sunt efectuate atunci când laptopul se alimentează de la baterie deoarece acestea necesită mai multe resurse de sistem și sporesc, implicit, consumul de energie.

BitDefender detectează când laptopul dumneavoastră a trecut pe baterie și intră automat în modul pentru laptop. De asemenea, BitDefender iese automat din modul pentru laptop, atunci când detectează că laptopul nu mai funcționează pe baterie.

Pentru a folosi Modul pentru laptop, trebuie să specificați în Asistentul de configurare că utilizați un laptop. Dacă nu ați selectat opțiunea potrivită la rularea asistentului, puteți activa Modul pentru laptop ulterior, după cum urmează:

1. Deschideți BitDefender.
2. Faceți clic pe butonul **Setări** din colțul din dreapta, sus al ferestrei.
3. În categoria Setări generale, selectați căsuța corespunzătoare opțiunii **Detecție Mod laptop**.
4. Faceți clic pe **OK** pentru a salva și aplica modificările.

6.7. Detecție automată unități

BitDefender detectează automat unitățile mobile de stocare pe care le conectați la calculator și propune scanarea lor înainte să accesați fișierele pe care le conțin acestea. Se recomandă pentru a preveni pătrunderea virușilor și a altor aplicații periculoase pe calculatorul dvs.

Unitățile detectate fac parte din următoarele categorii:

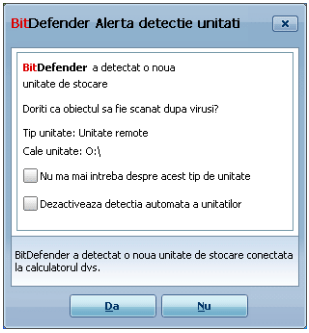
- CD/DVD
- unitate de stocare USB, cum ar fi memoriile flash sau hard discurile externe
- unități de rețea mapate (la distanță)

La detectarea unei astfel de unități se afișează o fereastră de alertă.

Pentru a scana unitatea de stocare, faceți clic pe **Da**. Va apărea programul asistent Scanare antivirus, care vă va ghida în procesul de scanare. Pentru informații detaliate despre acest program asistent, consultați secțiunea *„Programul asistent de scanare"* (p. 57).

Dacă nu doriți să scanați unitatea, faceți clic pe **Nu** . În acest caz, v-ar putea fi de folos una dintre aceste opțiuni:

- **Nu mă mai întreba despre acest tip de unitate** - BitDefender nu va mai propune



Alerta detecție unități

scanarea unităților de stocare de acest tip atunci când acestea sunt conectate la calculator.

- **Dezactivează detecția automată a unităților** - Nu vi se va mai propune să scanați noile unități de stocare atunci când acestea sunt conectate la calculator.

Dacă ați dezactivat detecția automată a unităților în mod accidental și vreți s-o reactivați sau să-i configurați setările, urmați acești pași:

1. Deschideți BitDefender și treceți interfața în Modul Expert.
2. Mergeți la **Antivirus>Scanare viruși**.
3. În lista de sarcini de scanare, localizați sarcina **Scanare detecție unități**.
4. Faceți clic-dreapta pe sarcină și selectați **Deschidere**. Va apărea o nouă fereastră.
5. Pe tabul **General**, configurați opțiunile de scanare după cum este necesar. Pentru mai multe informații, consultați secțiunea *„Configurarea setărilor de scanare”* (p. 144).
6. Pe tabul **Detecție**, alegeți tipurile de unități de stocare de detectat.
7. Faceți clic pe **OK** pentru a salva și aplica modificările.

7. Remediere probleme

BitDefender folosește un sistem de monitorizare pentru a detecta și a vă informa despre problemele care pot afecta securitatea calculatorului și a datelor dvs. În mod implicit, sunt monitorizate numai problemele considerate a fi foarte importante. Totuși, puteți configura sistemul după cum doriți, prin alegerea problemelor despre care doriți să primiți notificări.

Problemele în așteptare sunt semnalate astfel:

- Un simbol special este afișat deasupra iconiței BitDefender din bara de sistem pentru a semnala existența unor probleme în așteptare.

  Triunghi roșu cu semnul exclamării: Probleme grave de securitate afectează calculatorul dvs. Acestea necesită atenția dvs imediat și trebuie remediate în cel mai scurt timp.

  De asemenea, dacă treceți mouse-ul peste iconiță, o fereastră pop-up va confirma existența unor probleme în așteptare.

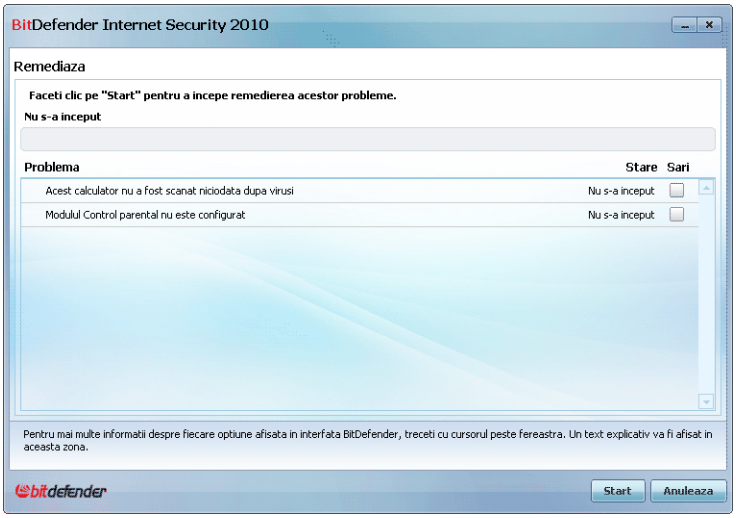
- Când deschideți BitDefender, zona de stare a securității va indica numărul de probleme care afectează sistemul dvs.

  - În Modul Intermediar, starea de securitate este afișată în tabul **Pagina de stare**.
  - În Modul Expert, mergeți la **General>Pagina de stare** pentru a verifica starea de securitate.

7.1. Asistent Remediere toate problemele

Cel mai ușor mod de a remedia problemele existente este să urmați pașii asistentului **Remediază problemele**. Asistentul vă ajută să înlăturați cu ușurință toate amenințările la adresa securității calculatorului și a datelor dvs. Pentru a deschide asistentul, aveți următoarele alternative:

- Faceți clic-dreapta pe iconița BitDefender din bara de sistem și selectați **Remediază**.
- Deschideți BitDefender. În funcție de modul de vizualizare a interfeței cu utilizatorul, procedați după cum urmează:
  - În Modul Novice, faceți clic pe **Remediază**.
  - În Modul Intermediar, mergeți la tabul **Stare** și faceți clic pe **Remediază**.
  - În Modul Expert, mergeți la tabul **General>Stare** și faceți clic pe **Remediază**.



Asistent Remediere toate problemele

Programul asistent afișează lista vulnerabilităților legate de securitatea calculatorului dvs.

Toate problemele actuale sunt selectate pentru a fi remediate. Dacă există o problemă care nu doriți să fie remediată, selectați căsuța corespunzătoare acesteia. Dacă faceți acest lucru, starea problemei în cauză va fi înlocuită cu **Omite**.

Notă

Dacă nu doriți să fiți informat despre anumite probleme, trebuie să configurați sistemul de monitorizare în consecință, conform instrucțiunilor din secțiunea următoare.

Pentru a rezolva problemele selectate, faceți clic pe **Start**. Unele probleme sunt remediate imediat.Pentru remedierea celorlalte, veți avea la dispoziție programe asistent.

Problemele pe care acest program asistent vă permite să le remediați pot fi grupate în următoarele categorii principale:

- **Setări de securitate dezactivate .** Aceste probleme sunt remediate pe loc, prin activarea setărilor de securitate în cauză.
- **Sarcini de securitate preventive pe care trebuie să le efectuați.** Un exemplu de astfel de sarcină este scanarea calculatorului. Este recomandat să vă scanați calculatorul cel puțin o dată pe săptămână. BitDefender va efectua această scanare automat, în majoritatea cazurilor. Dacă ați modificat programul

de scanare sau dacă acest program nu este finalizat, veți fi informat despre această problemă.

Când remediați aceste probleme, un program asistent vă ajută să finalizați sarcina cu succes.

- **Vulnerabilități ale sistemului.** BitDefender verifică automat dacă există vulnerabilități ale sistemului dvs și vă informează în legătură cu acestea. În categoria vulnerabilităților sistemului intră:
  - parolele simple ale conturilor de utilizator Windows.
  - programele neactualizate de pe calculatorul dvs.
  - actualizări Windows lipsă.
  - actualizările Windows automate dezactivate.

  Când apar astfel de probleme, se lansează programul asistent de scanare după vulnerabilități. Acesta vă permite să remediați vulnerabilitățile sistemului care au fost detectate. Pentru informații detaliate, consultați secțiunea *„Asistent Verificare vulnerabilități”* (p. 69).

7.2. Configurarea monitorizării problemelor

Sistemul de monitorizare a problemelor este preconfigurat să monitorizeze și să vă alerteze în legătură cu problemele care pot afecta securitatea calculatorului și a datelor dvs. Pot fi monitorizate și alte probleme, pe baza alegerilor pe care le faceți în cadrul programului asistent de configurare (când configurați profilul dvs de utilizator). În afară de problemele monitorizate în mod implicit, există o serie de alte probleme despre care puteți fi informat.

Puteți configura sistemul de monitorizare pentru ca acesta să corespundă cel mai bine nevoilor dvs de securitate prin alegerea anumitor probleme în legătură cu care doriți să fiți informat. Puteți face acest lucru fie în Modul Intermediar, fie în Modul Expert.

- În Modul Intermediar, sistemul de monitorizare poate fi configurat din locații diferite. Urmați pașii:
  1. Mergeți la **Securitate**, tabul **parental** sau **Seif pentru fișiere**.
  2. Faceți clic pe **Configurare monitorizare stare**.
  3. Selectați căsuțele corespunzătoare obiectelor care doriți să fie monitorizate.

  Pentru mai multe detalii, consultați secțiunea „Modul Intermediar” (p. 95) a acestui manual.
- În Modul Expert, sistemul de monitorizare poate fi configurat dintr-o singură locație. Urmați pașii:
  1. Mergeți la **General>Stare**.
  2. Faceți clic pe **Configurare monitorizare stare**.
  3. Selectați căsuțele corespunzătoare obiectelor care doriți să fie monitorizate.

Pentru informații detaliate, consultați capitolul *„Pagina de stare”* (p. 120).

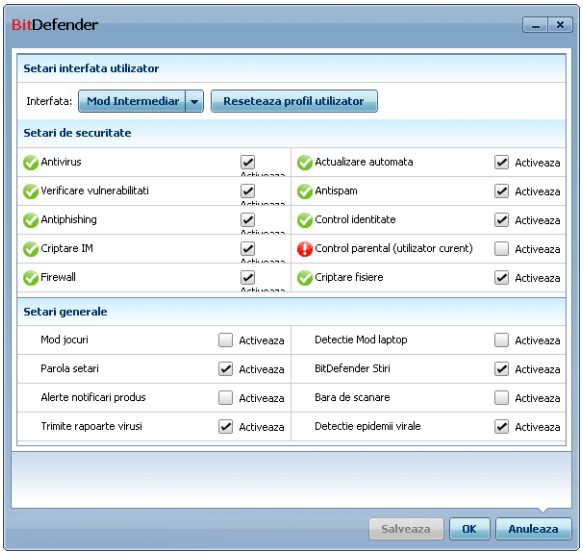
8. Configurarea setărilor de bază

Puteți să configurați setările principale de produs (inclusiv să schimbați modul de vizualizare a interfeței cu utilizatorul) din fereastra de setări de bază. Pentru a o deschide, aveți următoarele opțiuni:

- Deschideți BitDefender și faceți clic pe butonul **Setări** din colțul din dreapta-sus al ferestrei.
- Faceți clic-dreapta pe iconița BitDefender din bara de sistem și selectați **Setări de bază**.

Notă

Pentru configurarea detaliată a setărilor de produs, folosiți interfața în Modul Expert. Pentru mai multe detalii, consultați secțiunea „Modul Expert” (p. 119) a acestui manual.



Setări de bază

Setările sunt grupate în trei categorii:

- Setări interfață cu utilizatorul
- Setări securitate
- Setări generale

Pentru a aplica și a salva modificările de configurație pe care le faceți, faceți clic pe **OK**. Pentru a închide fereastra fără a salva modificările, faceți clic pe **Anulează**.

8.1. Setări interfață cu utilizatorul

În această zonă, puteți schimba modul de vizualizare al interfeței cu utilizatorul și reseta profilul utilizatorului.

Schimbarea modului de vizualizare a interfeței cu utilizatorul. . Conform descrierii din secțiunea *„Moduri de vizualizarea a interfeței cu utilizatorul”* (p. 24), există trei moduri de afișare a interfeței cu utilizatorul. Fiecare mod este este destinat unei anumite categorii de utilizatori, în funcție de aptitudinile lor de operare a calculatorului. Astfel, interfața cu utilizatorul corespunde nevoilor tuturor tipurilor de utilizatori, de la începători la experți în utilizarea calculatorului.

Primul buton arată modul actual de vizualizare a interfeței cu utilizatorul. Pentru a modifica modul de afișare a interfeței cu utilizatorul, faceți clic pe săgeata de pe buton și selectați modul dorit din meniu.

Mod	Descriere
Mod Novice	Potrivit pentru utilizatorii începători și pentru cei care doresc ca BitDefender să le protejeze calculatoarele și datele fără a fi solicitați să intervină. În acest mod, produsul este foarte ușor de utilizat, iar interacțiunea dvs cu el este minimă. Tot ce trebuie să faceți este să remediați problemele existente, atunci când sunt semnalate de BitDefender. Un program asistent intuitiv vă ghidează, pas cu pas, în acest proces. În plus, puteți efectua sarcini obișnuite, cum ar fi actualizarea semnăturilor de viruși din baza de date BitDefender și a fișierelor de produs, precum și scanarea calculatorului.
Mod Intermediar	Destinat utilizatorilor cu abilități medii de folosire a calculatorului, acest mod extinde capacitățile de acțiune oferite în Modul novice. Puteți remedia problemele separat și puteți alege care dintre acestea să fie monitorizate. În plus, puteți administra la distanță produsele BitDefender instalate pe calculatoarele din rețeaua personală.
Mod Expert	Potrivit pentru utilizatori mai experimentați, acest mod vă permite să configurați complet fiecare funcționalitate BitDefender. De asemenea, puteți folosi toate sarcinile disponibile pentru a vă proteja calculatorul și datele.

Resetarea profilului utilizatorului. Profilul utilizatorului reflectă principalele activități desfășurate pe calculator. În funcție de profil, interfața produsului este organizată astfel încât să vă permită să accesați ușor sarcinile dvs favorite.

Pentru a reconfigura profilul de utilizator, faceți clic pe **Resetează profil utilizator** și urmați pașii asistentului de configurare.

8.2. Setări de securitate

În această zonă, puteți activa sau dezactiva setările de produs care acoperă diverse aspecte ale securității calculatorului și a datelor. Starea curentă a unei setări este indicată prin una dintre aceste iconițe:

Cerc verde cu bifă: Setarea este activată.
Cerc roșu cu semnul exclamării: Setarea este dezactivată.

Pentru a activa/dezactiva o setare, selectați/deselectați căsuța **Activare** corespunzătoare.

Avertisment

Atenție când dezactivați protecția în timp real, firewallul sau actualizarea automată. Dezactivarea acestor funcționalități poate compromite securitatea calculatorului dumneavoastră. Dacă este necesar să le dezactivați, amintiți-vă să le activați din nou cât mai curând posibil.

Tabelul următor conține întreaga listă de setări și descrierea lor:

Setare	Descriere
Antivirus	Protecția în timp real asigură scanarea tuturor fișierelor accesate de dvs sau de o aplicație care rulează pe acest sistem.
Actualizare automată	Actualizarea automată asigură descărcarea și instalarea automată, în mod regulat, a celor mai recente fișiere de produs și semnături BitDefender.
Verificare vulnerabilități	Verificarea automată a vulnerabilităților asigură menținerea la zi a aplicațiilor critice de pe calculatorul dumneavoastră.
Antispam	Protecția Antispam filtrează mesajele e-mail pe care le primiți, marcându-le pe cele nedorite ca SPAM.
Antiphishing	Protecția antiphishing detectează și vă alertează în timp real dacă o pagină web este folosită pentru furt de informații personale.

Setare	Descriere
Control identitate	Controlul identității vă permite să împiedicați trimiterea de date cu caracter personal pe Internet, fără consimțământul dvs. Această opțiune blochează orice mesaj instant, e-mail sau formular web prin care se transmit către destinatari neautorizați (adrese) date pe care le-ați identificat ca având caracter personal.
Criptare IM	Criptarea mesageriei instant asigură confidențialitatea conversațiilor dvs prin Yahoo! Messenger și Windows Live Messenger cu interlocutori care folosesc un produs BitDefender și o aplicație de mesagerie instant compatibile.
Control parental	Controlul parental restricționează activitățile desfășurate pe calculator și online de către copii, pe baza regulilor definite de dvs. Restricțiile pot include blocarea accesului la site-uri web cu conținut inadecvat precum și limitarea accesului la jocuri și la Internet, în funcție de programul indicat.
Firewall	Firewallul vă protejează calculatorul de atacurile din exterior ale hackerilor și aplicațiilor periculoase.
Criptare fișiere	Opțiunea Criptare fișiere păstrează confidențialitatea documentelor dumneavoastră prin criptarea acestora în seifuri speciale. Dacă dezactivați opțiunea Criptare fișiere, toate seifurile pentru fișiere vor fi închise și nu veți mai avea acces la fișierele pe care acestea le conțin.

Starea unora dintre aceste setări poate fi monitorizată de sistemul BitDefender de monitorizare a problemelor. Dacă dezactivați o setare monitorizată, BitDefender va semnala acest lucru ca pe o problemă pe care trebuie s-o remediați.

Dacă nu doriți ca o setare monitorizată pe care ați dezactivat-o să fie semnalată ca problemă, trebuie să configurați sistemul de monitorizare în consecință. Puteți face acest lucru fie în Modul Intermediar, fie în Modul Expert.

- În Modul Intermediar, sistemul de monitorizare poate fi configurat din locații diferite, în funcție de categoriile de setări. Pentru mai multe detalii, consultați secțiunea „Modul Intermediar” (p. 95) a acestui manual.
- În Modul Expert, sistemul de monitorizare poate fi configurat dintr-o singură locație. Urmați pașii:
  1. Mergeți la **General>Stare**.
  2. Faceți clic pe **Configurare monitorizare stare**.

3. Deselectați căsuța corespunzătoare obiectului care nu doriți să fie monitorizat.

Pentru informații detaliate, consultați capitolul *„Pagina de stare”* (p. 120).

8.3. Setări generale

În această zonă, puteți activa sau dezactiva setările care afectează comportamentul produsului și interacțiunea cu utilizatorul. Pentru a activa/dezactiva o setare, selectați/deselectați căsuța **Activare** corespunzătoare.

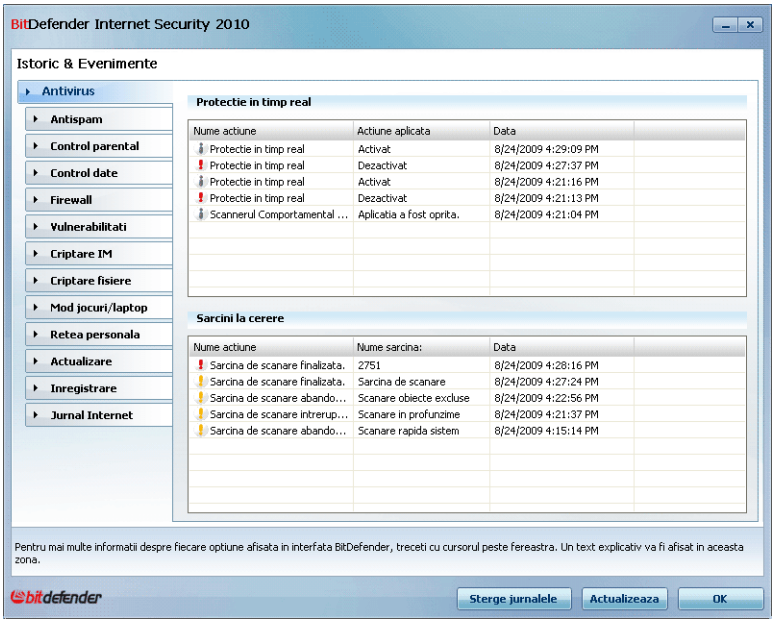
Tabelul următor conține întreaga listă de setări și descrierea lor:

Setare	Descriere
Mod pentru jocuri	Modul pentru jocuri modifică temporar setările de protecție pentru a minimiza impactul acestora asupra performanței sistemului atunci când vă jucați pe calculator.
Detecție mod pentru laptop	Modul pentru laptop modifică temporar setările de protecție pentru a minimiza impactul acestora asupra duratei de funcționare a laptopului pe baterie.
Parola pentru setări	Aceasta asigură că setările BitDefender pot fi modificate doar de către persoanele care cunosc această parolă. La activarea acestei opțiuni, vi se va cere să configurați parola de setări. Introduceți parola dorită în ambele câmpuri și faceți clic pe **OK** pentru a o seta.
Știri BitDefender	Activând această opțiune, veți primi știri importante legate de companie, actualizări de produs sau noi amenințări de securitate de la BitDefender.
Alerte de notificare produs	Activând această opțiune, veți primi alerte informative.
Bara de scanare	Bara de scanare este o fereastră mică, transparentă care indică progresul activității de scanare a BitDefender. Pentru mai multe informații, consultați secțiunea *„Bara de scanare”* (p. 33).
Trimite rapoarte viruși	Activând această opțiune, BitDefender va trimite rapoartele de scanare către Laboratorul BitDefender pentru analiză. Aceste rapoarte nu vor conține date confidențiale, cum ar fi numele dumneavoastră sau adresa IP și nu vor fi folosite în scop comercial.
Detecție epidemii virale	Activând această opțiune, BitDefender va trimite rapoarte privind potențiale epidemii virale către

Setare	Descriere
	Laboratorul BitDefender pentru analiză. Aceste rapoarte nu vor conține date confidențiale, cum ar fi numele dumneavoastră sau adresa IP, și nu vor fi folosite în scop comercial.

9. Istoric și evenimente

Linkul **Vizualizare jurnale**, situat în partea de jos a ferestrei BitDefender, deschide o nouă fereastră care conține istoricul &evenimentele BitDefender. Această fereastră vă furnizează un rezumat al evenimentelor legate de securitate. De exemplu, puteți verifica rapid dacă produsul a fost actualizat, dacă au fost detectate aplicații malițioase pe calculatorul dumneavoastră etc.



Evenimente

Pentru a gestiona mai ușor istoricul și evenimentele BitDefender, următoarele categorii sunt oferite în partea stângă:

- **Antivirus**
- **Antispam**
- **Control parental**
- **Control date**
- **Firewall**
- **Vulnerabilitate**
- **Criptare IM**
- **Criptare fișiere**
- **Mod jocuri/laptop**

- **Rețea personală**
- **Actualizare**
- **Înregistrare**
- **Jurnal Internet**

Pentru fiecare categorie este disponibilă o listă de evenimente. Următoarele informații sunt furnizate pentru fiecare eveniment: o scurtă descriere, acțiunea luată de BitDefender atunci când evenimentul a avut loc și data și timpul când a avut loc. Dacă doriți mai multe informații în legătură cu un anumit eveniment din listă, faceți dublu-clic pe evenimentul respectiv.

Faceți clic pe **Șterge jurnalele** dacă doriți să ștergeți înregistrările vechi sau pe **Actualizează** pentru a vă asigura că sunt afișate și cele mai recente înregistrări.

10. Înregistrare și Contul meu

Perioada de evaluare a BitDefender Internet Security 2010 este de 30 de zile. În perioada de evaluare, produsul este complet funcțional și îl puteți testa pentru a vedea dacă este în conformitate cu așteptările dumneavoastră. Vă rugăm să rețineți că, după 15 de zile de evaluare, produsul va înceta să mai efectueze actualizări dacă nu creați un cont BitDefender. Crearea unui cont BitDefender este o parte obligatorie a procesului de înregistrare.

Înainte de încheierea perioadei de evaluare, trebuie să înregistrați produsul pentru a vă proteja calculatorul în continuare. Procedura de înregistrare cuprinde două etape:

1. **Activarea produsului (înregistrarea unui cont BitDefender).** Trebuie să creați un cont BitDefender pentru ca produsul să se actualizeze și pentru a avea acces la suport tehnic gratuit. Dacă aveți deja un cont BitDefender, trebuie să vă înregistrați produsul BitDefender pe acel cont. BitDefender vă va înștiința că trebuie să vă activați produsul și vă va ajuta să remediați această problemă.

   Important

   Este necesar să vă creați un cont în termen de 15 zile de la instalarea BitDefender (dacă înregistrați produsul cu o serie de înregistrare, termenul limită se extinde la 30 de zile). În caz contrar, BitDefender nu se va mai actualiza.

2. **Înregistrarea cu o serie de înregistrare.** Seria de înregistrare precizează pentru cât timp aveți dreptul de a utiliza produsul. Imediat după expirarea seriei de înregistrare, BitDefender se va opri din funcționare și nu vă va mai proteja calculatorul. Trebuie să vă înregistrați produsul cu o serie de înregistrare atunci când se încheie perioada de evaluare. Este recomandat să achiziționați o serie de înregistrare sau să vă reînnoiți licența cu câteva zile înainte de expirarea seriei actuale de înregistrare.

10.1. Înregistrarea BitDefender Internet Security 2010

Dacă doriți să înregistrați produsul cu o serie de înregistrare sau să schimbați seria de licență actuală, faceți clic pe linkul **Înregistrare**, situat în partea de jos a ferestrei BitDefender. Va apărea fereastra de înregistrare a produsului.

Înregistrare

Puteți vedea starea de înregistrare a produsului dumneavoastră BitDefender, seria curentă de înregistrare și câte zile au mai rămas până la expirarea licenței.

Pentru a înregistra BitDefender Internet Security 2010:

1. Introduceți seria de înregistrare în câmpul editabil.

   Notă
   Puteți găsi seria dumneavoastră de înregistrare:
   - pe eticheta de pe CD.
   - pe certificatul de înregistrare al produsului.
   - în e-mailul de achiziționare online.

   Dacă nu aveți o serie de înregistrare BitDefender, faceți clic pe linkul furnizat pentru a merge la magazinul online BitDefender și a cumpăra una.

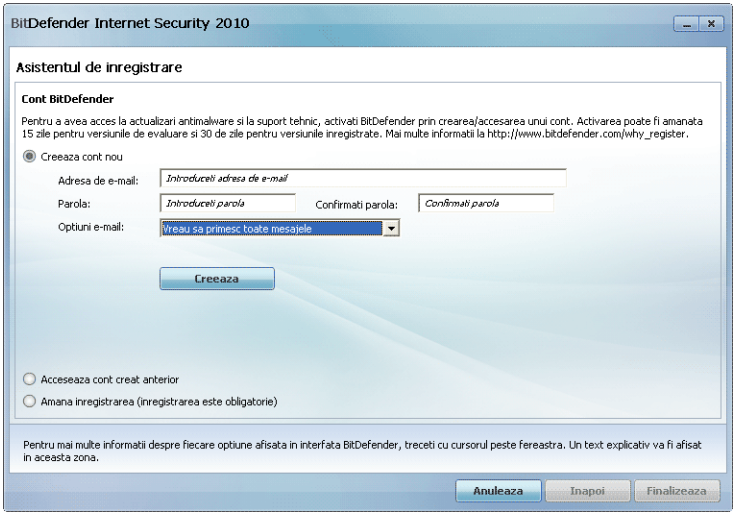
2. Faceți clic pe **Înregistrare**.
3. Faceți clic pe **Finalizare**.

10.2. Activarea BitDefender

Pentru a activa BitDefender, trebuie să creați sau să accesați un cont BitDefender. Dacă nu ați înregistrat un cont BitDefender în cursul programului asistent inițial de înregistrare, aveți următoarele alternative:

- În Modul Novice, faceți clic pe **Remediază**. Asistentul vă va permite să remediați toate problemele în așteptare, inclusiv activarea produsului.
- În Modul Intermediar, mergeți la tabul **Securitate** și faceți clic pe butonul **Remediază** corespunzător problemei legate de activarea produsului.
- În Modul Expert, mergeți la **Înregistrare** și faceți clic pe butonul **Activare produs**.

Se va deschide fereastra de înregistrare a contului. Aici puteți crea sau vă puteți conecta la un cont BitDefender pentru a vă activa produsul.



Creare cont

Dacă nu doriți să creați un cont BitDefender în acest moment, selectați **Amână înregistrarea** si faceți clic pe **Finalizează**. Altfel, continuați în funcție de situația dumneavoastră actuală:

- „Nu am un cont BitDefender” (p. 54)
- „Deja am un cont BitDefender” (p. 55)

Important

Este necesar să vă creați un cont în termen de 15 zile de la instalarea BitDefender (dacă înregistrați produsul cu o serie de înregistrare, termenul limită se extinde la 30 de zile). În caz contrar, BitDefender nu se va mai actualiza.

Nu am un cont BitDefender

Pentru a crea un cont BitDefender, urmați acești pași:

1. Selectați **Creează cont nou**.
2. Introduceți informațiile solicitate în câmpurile corespunzătoare. Informațiile furnizate aici vor rămâne confidențiale.
   - **Adresă de e-mail** - introduceți adresa dvs. de e-mail.
   - **Parolă** - introduceți o parolă pentru contul dumneavoastră BitDefender. Parola trebuie să conțină între 6 și 16 caractere.
   - **Confirmați parola** - introduceți parola din nou.

   Notă
   După activarea contului, puteți folosi adresa de e-mail și parola furnizate pentru a-l accesa, la adresa http://myaccount.bitdefender.com.

3. Opțional, BitDefender vă poate informa despre oferte speciale și promoții folosind adresa de e-mail a contului dumneavoastră. Selectați una dintre opțiunile disponibile din meniu:
   - **Vreau sa primesc toate mesajele**
   - **Vreau sa primesc numai mesaje despre produs**
   - **Nu vreau sa primesc niciun mesaj**
4. Faceți clic pe **Creează**.
5. Faceți clic pe **Finalizează** pentru a încheia programul asistent.
6. **Activați-vă contul.** Pentru a vă putea utiliza contul, trebuie mai întâi să îl activați. Verificați-vă adresa de e-mail și urmați instrucțiunile din mesajul trimis de către serviciul de înregistrare BitDefender.

Deja am un cont BitDefender

BitDefender va detecta automat dacă ați creat anterior un cont BitDefender pe calculatorul dumneavoastră. În acest caz, furnizați parola contului dvs și faceți clic pe **Accesează**. Faceți clic pe **Finalizează** pentru a încheia programul asistent.

Dacă aveți deja un cont activ, dar BitDefender nu-l detectează, urmați pașii de mai jos pentru a înregistra produsul cu contul respectiv:

1. Selectați **Accesează cont creat anterior**.
2. Introduceți adresa de e-mail și parola contului dvs în câmpurile corespunzătoare.

   Notă
   Dacă v-ați uitat parola, faceți clic pe **V-ați uitat parola?** și urmați instrucțiunile.

3. Opțional, BitDefender vă poate informa despre oferte speciale și promoții folosind adresa de e-mail a contului dumneavoastră. Selectați una dintre opțiunile disponibile din meniu:

- **Vreau sa primesc toate mesajele**
- **Vreau sa primesc numai mesaje despre produs**
- **Nu vreau sa primesc niciun mesaj**

4. Faceți clic pe **Accesează**.
5. Faceți clic pe **Finalizează** pentru a încheia programul asistent.

10.3. Achiziționarea unei licențe

Dacă perioada de evaluare se va încheia în curând, trebuie să achiziționați o serie de înregistrare și să vă înregistrați produsul. Deschideți BitDefender și faceți clic pe linkul **Cumpără**, situat în partea de jos a ferestrei. Acest link vă duce la o pagină web de unde puteți achiziționa o serie de înregistrare pentru produsul dumneavoastră BitDefender.

10.4. Reînnoirea licenței

La reînnoirea licenței, clienții BitDefender beneficiază de o reducere. În plus, este posibilă actualizarea produsului la versiunea curentă beneficiind de o altă reducere sau chiar gratuit.

Dacă seria actuală de înregistrare va expira în curând, trebuie să vă reînnoiți licența. Deschideți BitDefender și faceți clic pe linkul **Cumpără**, situat în partea de jos a ferestrei. Acest link vă duce la o pagină web unde vă puteți reînnoi licența.

11. Asistenți

Pentru a putea folosi BitDefender foarte ușor, aveți la dispoziție o serie de programe asistent care vă permit să efectuați anumite sarcini de securitate sau să configurați setări de produs complexe. Acest capitol conține o descriere a programelor asistent care pot apărea atunci când remediați probleme sau efectuați sarcini specifice cu BitDefender. Alte programe asistent de configurare sunt descrise separat, în secțiunea „Modul Expert” (p. 119).

11.1. Programul asistent de scanare

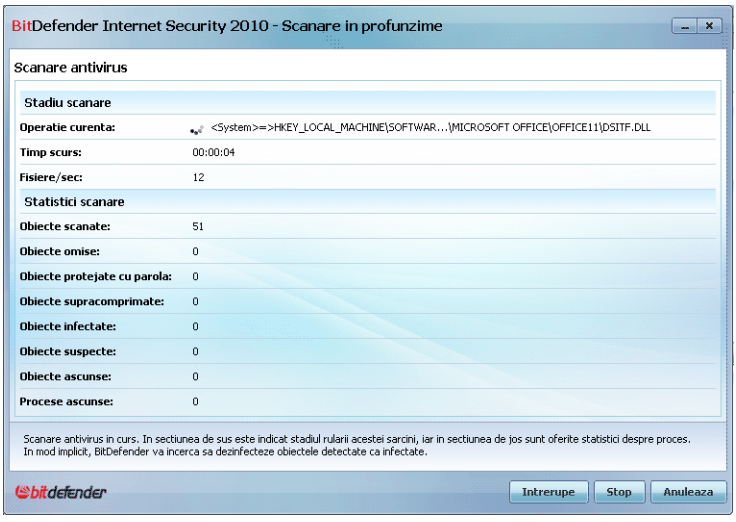
Atunci când inițiați o scanare la cerere (de exemplu, faceți clic-dreapta pe un director și selectați **Scanează cu BitDefender**), va apărea programul asistent de scanare. Urmați programul asistent în trei pași pentru a realiza procesul de scanare.

Notă

Dacă asistentul de scanare nu apare, este posibil ca scanarea să fie configurată să ruleze discret, în fundal. Căutați iconița de scanare în curs în bara de sistem. Puteți face dublu-clic pe această iconiță pentru a deschide fereastra de scanare și a vedea evoluția scanării.

11.1.1. Pasul 1/3 - Scanare

BitDefender va începe scanarea obiectelor selectate.



Scanare

Puteți vedea stadiul și statisticile scanării (viteza de scanare, timpul scurs de la începutul scanării, numărul obiectelor scanate / infectate / suspecte / ascunse și altele).

Așteptați ca BitDefender să finalizeze scanarea.

Notă
Procesul de scanare poate dura destul de mult, în funcție de complexitatea scanării.

Arhive protejate prin parolă. Dacă BitDefender detectează o arhivă protejată prin parolă în timpul scanării și acțiunea implicită este **Cere parola**, vi se va solicita să furnizați parola. Arhivele protejate prin parolă nu pot fi scanate decât dacă furnizați parola. Următoarele opțiuni sunt disponibile:

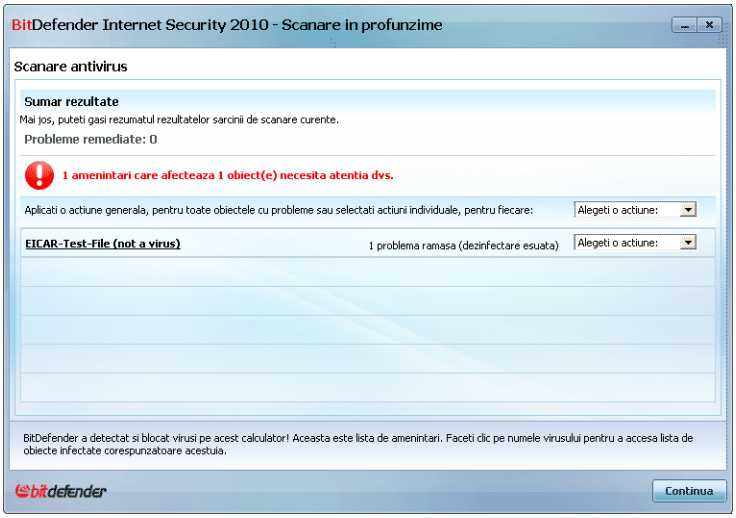
- **Doresc să introduc parola pentru acest obiect.** Dacă doriți ca BitDefender să scaneze arhiva, selectați această opțiune și introduceți parola. Dacă nu cunoașteți parola, selectați una dintre celelalte opțiuni.
- **Nu vreau să introduc parola pentru acest obiect (nu scana acest obiect).** Selectând această opțiune, arhiva nu fi scanată.
- **Nu vreau să introduc parolă pentru niciun obiect (nu scana niciun obiect protejat prin parolă).** Selectați această opțiune dacă doriți să nu vi se mai solicite introducerea parolei pentru arhivele protejate prin parolă. BitDefender nu le va putea scana, dar va păstra o înregistrare în raportul de scanare.

Faceți clic pe **OK** pentru a continua scanarea.

Oprirea sau întreruperea temporară a scanării. Puteți opri scanarea oricând doriți făcând clic pe **Stop&Da**. Veți sări direct la ultimul pas al programului asistent. Pentru a opri temporar procesul de scanare, faceți clic pe **Întrerupe**. Va trebui să faceți clic pe **Reia** pentru a relua scanarea.

11.1.2. Pasul 2/3 - Selectați acțiunile

După ce scanarea a fost finalizată, va apărea o nouă fereastră, unde puteți vedea rezultatele scanării.



Acțiuni

Puteți vedea numărul problemelor care vă afectează sistemul.

Obiectele infectate sunt afișate în grupuri, în funcție de codul malware cu care sunt infectate. Faceți clic pe linkul corespunzător unei amenințări pentru a afla mai multe informații despre obiectele infectate.

Puteți alege o acțiune globală care să fie luată asupra tuturor problemelor sau puteți alege acțiuni separate pentru fiecare grup de probleme.

Una sau mai multe dintre opțiunile următoare pot apărea în meniu:

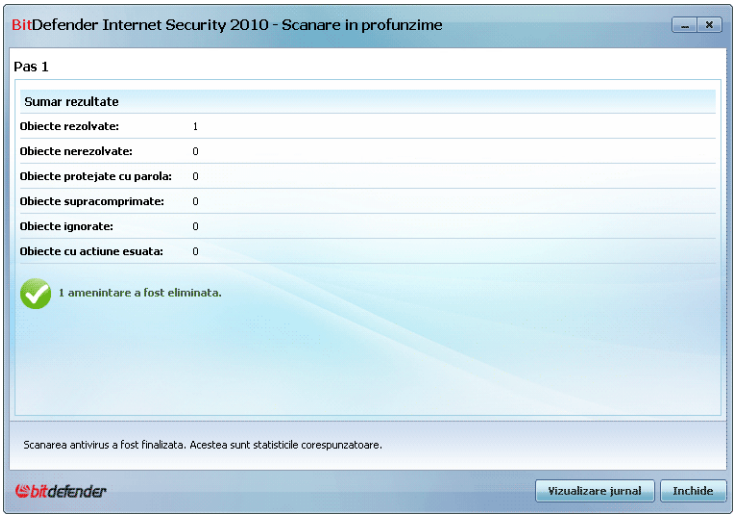
Acțiune	Descriere
Nicio acțiune	Nu se va lua nicio acțiune asupra fișierelor detectate. După finalizarea scanării, puteți deschide raportul de scanare pentru a vedea informații despre aceste fișiere.
Dezinfectează	Elimină codul malițios din fișierele infectate.
Șterge	Șterge fișierele detectate.
Mută în carantină	Mută fișierele detectate în carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.
Redenumește	Redenumește fișierele ascunse adăugând extensia `.bd.ren` la numele acestora. Ca urmare, veți putea

Acțiune	Descriere
	căuta și găsi astfel de fișiere pe calculatorul dumneavoastră, dacă există. Aceste fișiere ascunse nu sunt fișierele pe care le ascundeți deliberat din Windows. Ele sunt fișiere ascunse cu ajutorul unor programe speciale, cunoscute sub numele de rootkituri. Rootkiturile nu sunt în sine programe malițioase. Totuși, ele sunt utilizate frecvent pentru a împiedica detectarea virușilor sau aplicațiilor spion de către programele antivirus obișnuite.

Faceți clic pe **Continuă** pentru a aplica acțiunile specificate.

11.1.3. Pasul 3/3 - Examinați rezultatele

Atunci când BitDefender a remediat toate problemele apărute, rezultatele scanării vor fi afișate într-o nouă fereastră.



Rezumat

Puteți vedea un rezumat al rezultatelor. Dacă doriți informații complete cu privire la procesul de scanare, faceți clic pe **Jurnal** pentru a vizualiza raportul de scanare.

Important
Dacă este necesar, reporniți sistemul pentru a finaliza procesul de curățare.

Faceți clic pe **Închide** pentru a închide fereastra.

BitDefender nu a putut remedia anumite probleme

În majoritatea cazurilor, BitDefender va dezinfecta fișierele infectate detectate sau va izola infecția. Cu toate acestea, există anumite probleme care nu pot fi rezolvate.

În aceste cazuri, vă recomandăm să contactați echipa de suport a BitDefender pe pagina web www.bitdefender.ro. Reprezentanții noștri de suport tehnic vă vor ajuta să rezolvați problemele cu care vă confruntați.

BitDefender a detectat fișiere suspecte

Fișierele suspecte sunt fișiere detectate în cadrul analizei euristice ca fiind posibil infectate cu malware a cărui semnătură nu a fost încă lansată.

Dacă au fost detectate fișiere suspecte în timpul scanării, vi se va cere să le trimiteți laboratorului BitDefender. Faceți clic pe **OK** pentru a trimite aceste fișiere Laboratorului BitDefender spre a fi analizate.

11.2. Asistent scanare personalizată

Asistentul de scanare personalizată vă permite să creați și să rulați o sarcină de scanare la cerere și, opțional, s-o salvați ca Sarcină rapidă accesibilă atunci când folosiți BitDefender în Modul Intermediar.

Pentru a rula o sarcină de scanare personalizată folosind Asistentul de scanare personalizată, urmați acești pași:

1. În Modul Intermediar, mergeți la tabul **Securitate**.
2. În zona Sarcini rapide, faceți clic pe **Scanare personalizată**.
3. Urmați programul asistent în șase pași pentru a finaliza procesul de scanare.

11.2.1. Pasul 1/6 - Fereastră de întâmpinare

Bine ați venit!

Fereastra de întâmpinare

Dacă doriți să săriți peste această fereastră la rularea ulterioară a acestui asistent, selectați căsuța **Nu arăta acest pas la următoarea rulare a acestui asistent**.

Faceți clic pe **Înainte**.

11.2.2. Pasul 2/6 - Selectați locația

Aici puteți specifica fișierele sau directoarele de scanat, precum și opțiunile de scanare.

Selectare țintă

Faceți clic pe **Adaugă locație**, selectați fișierele sau directoarele pe care doriți să le scanați și faceți clic pe **OK**. Căile către locațiile selectate vor apărea în coloana **Țintă scanare** Dacă vă răzgândiți în legătură cu locația, faceți clic pe butonul **Șterge** de lângă aceasta. Faceți clic pe butonul **Elimină toate** pentru a elimina toate locațiile care au fost adăugate pe lista.

După ce ați selectat toate locațiile, setați **Opțiunile de scanare**. Opțiunile disponibile sunt:

Opțiune	Descriere
Scanează toate fisierele	Selectați această opțiune pentru a scana toate fișierele din directoarele selectate.
Scanează numai aplicațiile	Nu vor fi scanate decât fișierele program, și anume fișierele cu următoarele extensii: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml` și `.nws`.

Opțiune	Descriere
Scanează numai extensiile definite de utilizator	Nu vor fi scanate decât fișierele cu extensiile specificate de utilizator. Aceste extensii trebuie separate prin ";".

Faceți clic pe **Înainte**.

11.2.3. Pasul 3/6 - Selectați acțiunile

Aici puteți indica setările și nivelul de scanare.

Selectare acțiuni

- Selectați acțiunile care trebuie aplicate fișierelor infectate și suspecte detectate. Următoarele opțiuni sunt disponibile:

Acțiune	Descriere
Nicio acțiune	Nici se va efectua nici o acțiune în legătură cu fișierelor infectate. Aceste fișiere vor apărea în fișierul de raport.
Dezinfectează	Elimină codul malware din fișierele infectate detectate.

Acțiune	Descriere
Șterge	Șterge imediat fișierele infectate, fără niciun avertisment.
Mută în carantină	Mută fișierele infectate în carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.

- Selectați acțiunea care va fi aplicată fișierelor ascunse (rootkituri) detectate. Următoarele opțiuni sunt disponibile:

Acțiune	Descriere
Nicio acțiune	Nicio acțiune nu va fi aplicată fișierelor ascunse. Aceste fișiere vor apărea în fișierul de raport.
Redenumește	Redenumește fișierele ascunse adăugând extensia `.bd.ren` la numele acestora. Ca urmare, veți putea căuta și găsi astfel de fișiere pe calculatorul dumneavoastră, dacă există.

- Configurați agresivitatea scannerului. Aveți la dispoziție 3 niveluri. Trageți cursorul pe scală pentru a stabili nivelul adecvat de protecție:

Nivel de scanare	Descriere
Permisiv	Se scanează numai aplicațiile și numai după viruși. Nivelul de resurse consumate este redus.
Standard	Nivel moderat de resurse consumate. Toate fișierele sunt scanate după viruși și după programe spion.
Agresiv	Toate fișierele (inclusiv arhivele) sunt scanate împotriva virușilor și a aplicațiilor spion. Fișierele și procesele ascunse sunt incluse în procesul de scanare. Nivelul consumului de resurse este mai mare.

Utilizatorii avansați ar putea fi interesați să folosească setările de scanare oferite de BitDefender. Scannerul poate fi setat să caute anumite aplicații periculoase. Aceasta poate reduce semnificativ durata scanării și poate îmbunătăți viteza de reacție a calculatorului dvs în timpul scanării.

Trageți cursorul pentru a selecta **Personaliazare** și apoi faceți clic pe butonul **Nivel personal**. Va apărea o fereastră. Precizați tipul de aplicații periculoase

împotriva cărora doriți ca BitDefender să efectueze scanarea prin selectarea opțiunilor pe care le doriți:

Opțiune	Descriere
Scanează după viruși	Scanează după viruși cunoscuți. BitDefender detectează, de asemenea, și corpurile incomplete de viruși, îndepărtând astfel orice posibilă amenințare ce ar putea afecta securitatea sistemului dumneavostră.
Scanează după adware	Scanează după amenințări adware. Fișierele detectate vor fi considerate ca fiind infectate. Programele care includ componente adware se pot opri din funcționare dacă această opțiune este activată.
Scanează după spyware	Scanează după amenințări spyware cunoscute. Fișierele detectate vor fi considerate ca fiind infectate.
Scanează după applications	Scanează după aplicații legitime care pot fi folosite pentru a spiona, pentru a ascunde aplicații malițioase sau cu alte intenții răuvoitoare.
Scanează după dialere	Scanează după aplicații care apelează numere cu cost ridicat. Fișierele detectate vor fi considerate ca fiind infectate. Programele care includ componente adware se pot opri din funcționare dacă această opțiune este activată.
Scanare după rootkituri	Scanează după obiecte ascunse (fișiere și procese), cunoscute sub denumirea generică de rootkituri.
Scanează după keyloggers	Scanează după aplicații periculoase care înregistrează combinațiile de taste folosite.

Faceți clic pe **OK** pentru a închide fereastra.

Faceți clic pe **Înainte**.

11.2.4. Pasul 4/6 - Setări suplimentare

Înainte de începutul scanării, sunt disponibile opțiuni suplimentare:

Setări suplimentare

- Pentru a salva sarcina personalizată pe care o creați astfel încât s-o puteți folosi ulterior, selectați căsuța **Afișează sarcina în Modul Intermediar** și introduceți numele sarcinii în câmpul editabil.

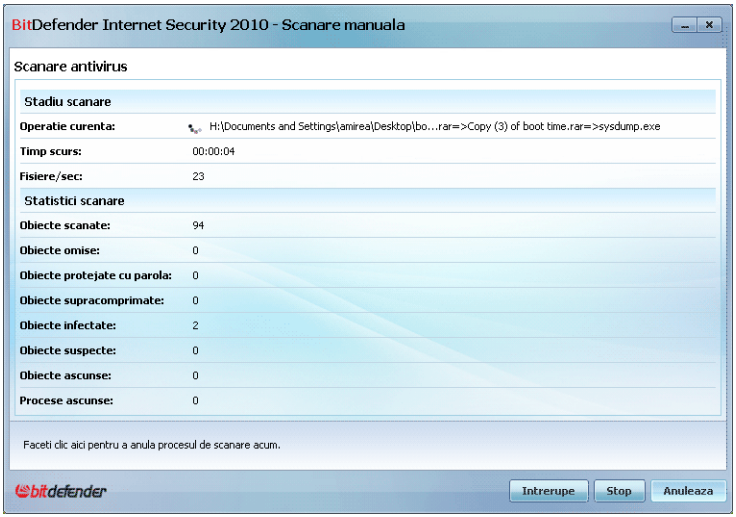
  Sarcina va fi adăugată pe lista de Sarcini rapide deja existentă în tabul Securitate și va apărea, de asemenea, în **Modul expert > Antivirus > Scanare viruși**.

- Pentru a închide calculatorul la finalul scanării, selectați căsuța **Închide calculatorul la finalul scanării, dacă nu este detectată nicio amenințare**.

Faceți clic pe **Pornire scanare**.

11.2.5. Pasul 5/6 - Scanare

BitDefender va începe scanarea obiectelor selectate:



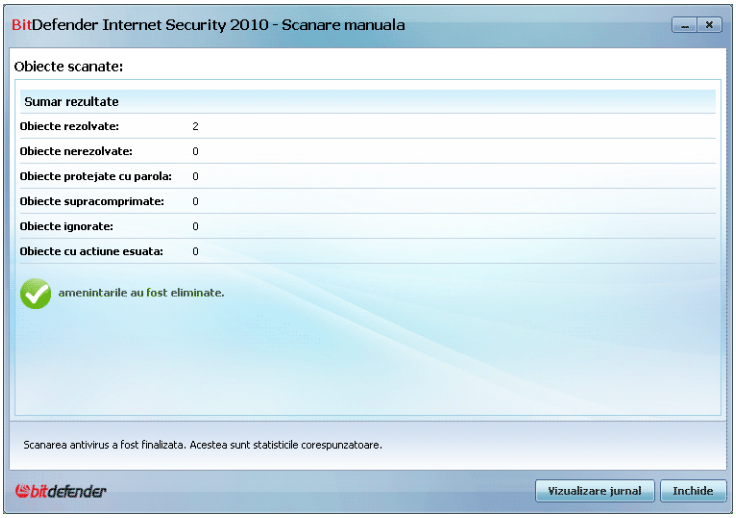
Scanare

Notă

Procesul de scanare poate dura destul de mult, în funcție de complexitatea scanării. Puteți face clic pe iconița de scanare în curs din bara de sistem pentru a deschide fereastra de scanare și a vedea stadiul procesului.

11.2.6. Pasul 6/6 - Examinați rezultatele

Când BitDefender a finalizat procesul de scanare, rezultatele acestuia vor apărea într-o fereastră nouă:



Rezumat

Puteți consulta sumarul rezultatelor. Dacă doriți informații complete cu privire la procesul de scanare, faceți clic pe **Jurnal** pentru a vizualiza jurnalul de scanare.

Important
Dacă este necesar, reporniți sistemul pentru a finaliza procesul de curățare.

Faceți clic pe **Închide** pentru a închide fereastra.

11.3. Asistent Verificare vulnerabilități

Acest program asistent verifică dacă există vulnerabilități ale sistemului și vă ajută să le remediați.

11.3.1. Pasul 1/6 - Selectați vulnerabilitățile de verificat

Vulnerabilități

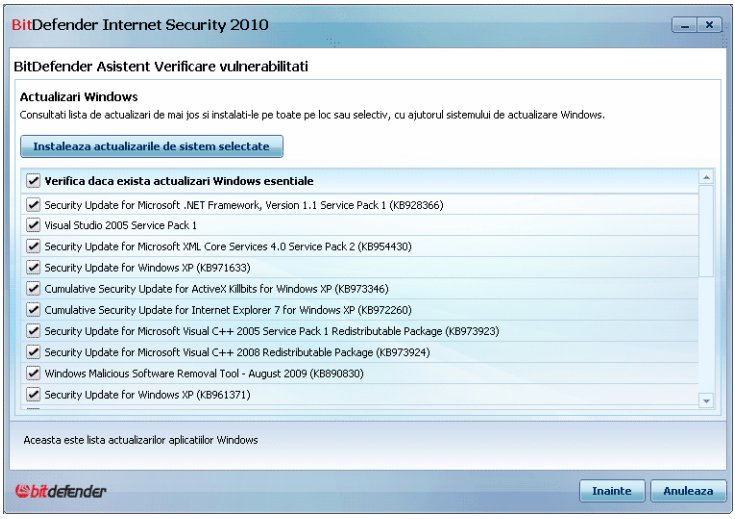
Faceți clic pe **Înainte** pentru a verifica sistemul după vulnerabilitățile selectate.

11.3.2. Pasul 2/6 - Căutare vulnerabilități

Căutare vulnerabilități

Așteptați ca BitDefender să finalizeze căutarea.

11.3.3. Pasul 3/6 - Actualizați Windows



Actualizări Windows

Puteți vedea lista actualizărilor critice și normale pentru Windows care nu sunt instalate pe calculatorul dumneavoastră. Faceți clic pe **Instalează toate actualizările de sistem** pentru a instala toate actualizările disponibile.

Faceți clic pe **Înainte**.

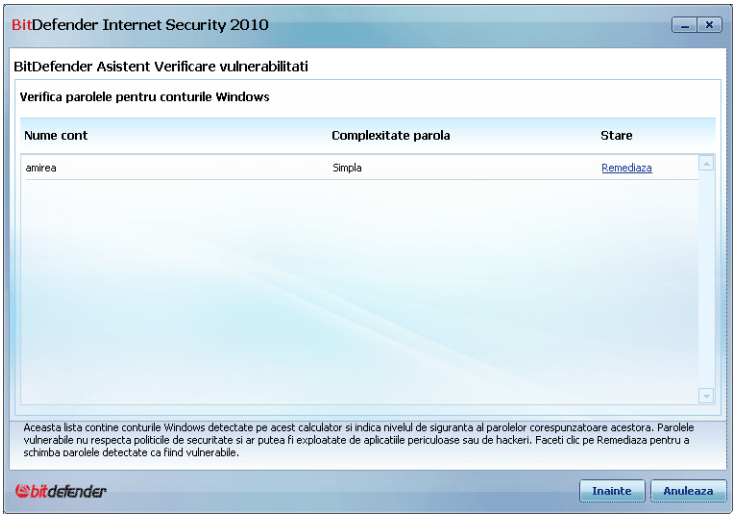
11.3.4. Pasul 4/6 - Actualizați aplicații

Aplicații

Puteți vedea lista aplicațiilor verificate de BitDefender și dacă acestea sunt la zi. Dacă o aplicație nu este la zi, faceți clic pe linkul furnizat pentru a descărca ultima versiune a acesteia.

Faceți clic pe **Înainte**.

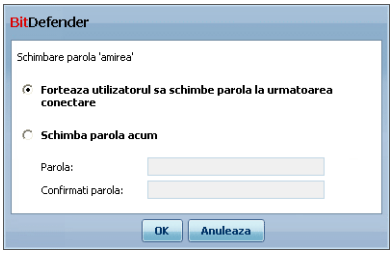
11.3.5. Pasul 5/6 - Schimbați parolele simple



Parole utilizatori

Puteti vedea lista conturilor de utilizator Windows configurate pe calculatorul dumneavoastră și de nivelul de protecție asigurat de parola acestora. O parolă poate fi **complexă** (greu de ghicit) sau **simplă** (ușor de descoperit de către persoane răuvoitoare dotate cu programe specializate).

Faceți clic pe **Remediază** pentru a modifica parolele slabe. Va apărea o nouă fereastră.



Schimbare parolă

Selectați metoda de rezolvare a acestei probleme:

- **Forțează utilizatorul să schimbe parola la următoarea conectare.** BitDefender va cere utilizatorului să schimbe parola data viitoare când acesta se conectează la contul său Windows.
- **Schimbă parola utilizatorului.** Trebuie să introduceți noua parolă în câmpurile editabile. Informați utilizatorul despre schimbarea parolei.

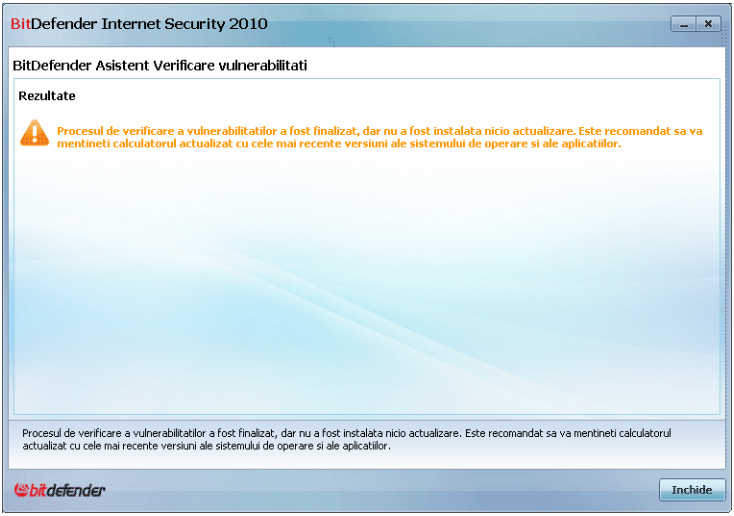
Notă

Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @). Puteți căuta pe Internet mai multe informații și sfaturi cu privire la crearea de parole complexe.

Faceți clic pe **OK** pentru a salva parola.

Faceți clic pe **Înainte**.

11.3.6. Pasul 6/6 - Examinați rezultatele



Rezultate

Faceți clic pe **Închide**.

11.4. Asistenți Seif pentru fișiere

Asistenții Seif pentru fișiere vă permit să creați și să administrați seifurile pentru fișiere BitDefender. Seiful pentru fișiere este un spațiu de stocare criptat de pe

calculatorul dvs, în care puteți păstra în siguranță fișiere, documente și chiar directoare importante.

Acești asistenți nu apar atunci când remediați probleme, pentru că păstrarea în seifurile pentru fișiere este o metodă opțională de protejare a datelor dvs. Asistenții nu pot fi lansați decâ din Interfața Intermediară, tabul **Stocare fișiere**, după cum urmează:

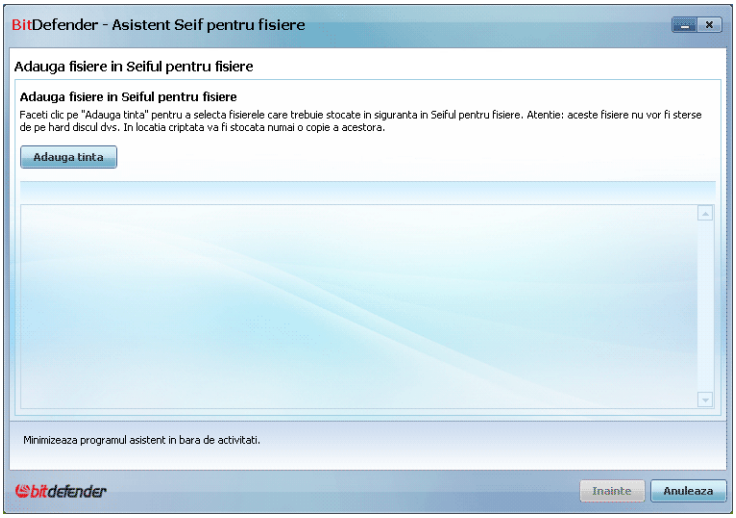
- **Adaugă fișier în seif** - pornește programul asistent care vă permite să stocați în siguranță fișierele / documentele dumneavoastră importante criptându-le în partiții special, securizate (seife de fișiere).
- **Șterge fișiere din seif** - pornește programul asistent care vă permite să ștergeți date din seiful de fișiere.
- **Vizualizare seif** - pornește programul asistent care vă permite să vedeți conținutul seifurilor dvs pentru fișiere.
- **Închidere seif** - pornește programul asistent care vă permite să vă închideți un seif deschis, pentru a proteja conținutul acestuia.

11.4.1. Adăugarea fișierelor în seif

Acest program asistent vă ajută să creați un seif pentru fișiere și să adăugați fișiere în el pentru a le stoca în siguranță pe calculatorul dvs.

Pasul 1/6 - Selectați locația

Aici puteți specifica fișierele și directoarele care să fie adăugate în seif.



Țintă

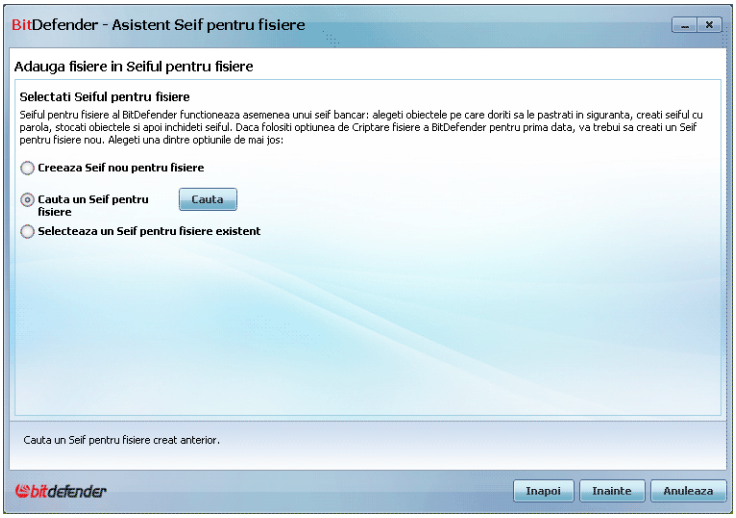
Faceți clic pe **Adaugă locație**, selectați fișierul sau directorul care doriți să fie adăugat și faceți clic pe **OK**. Calea către locația selectată va apărea în coloana **Cale**. Dacă vă răzgândiți în legătură cu locația, faceți clic pe butonul **Șterge** de lângă aceasta.

Notă
Puteți selecta una sau mai multe locații.

Faceți clic pe **Înainte**.

Pasul 2/6 - Selectați seiful

Aici puteți crea un nou seif sau puteți selecta un seif existent.



Selectați seiful

Dacă selectați **Caută un seif de fișiere**, trebuie să faceți clic pe **Caută** și să selectați seiful de fișiere. Veți merge la pasul 5 dacă seiful selectat este deschis sau la pasul 4 dacă este închis.

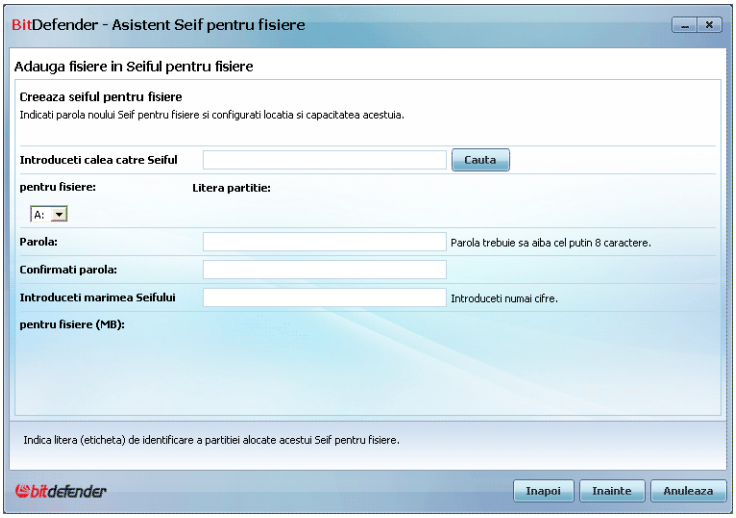
Dacă faceți clic pe **Selectează un seif de fișiere existent**, trebuie să faceți clic apoi pe numele seifului dorit. Veți merge la pasul 5 dacă seiful selectat este deschis sau la pasul 4 dacă este închis.

Selectați **Creează un nou seif de fișiere** dacă niciunul dintre seifurile existente nu corespunde nevoilor dumneavoastră. Veți merge la pasul 3.

Faceți clic pe **Înainte**.

Pasul 3/6 - Creați seiful

Aici puteți specifica informații referitoare la noul seif.



Creați seiful

Pentru a furniza informațiile necesare creării seifului de fișiere, urmați acești pași:

1. Faceți clic pe **Caută** și alegeți o locație pentru fișierul bvd.

   Notă
   Amintiți-vă că seiful de fișiere este de fapt un fișier criptat de pe calculatorul dumneavoastră, având extensia bvd.

2. Selectați o literă pentru partiția aferentă noului seif de fișiere din meniul corespunzător.

   Notă
   Amintiți-vă că atunci când deschideți fișierul bvd, va apărea o nouă partiție logică (un nou drive).

3. Introduceți parola pentru seiful de fișiere în câmpul corespunzător.

   Notă
   Parola trebuie să conțină minim 8 caractere.

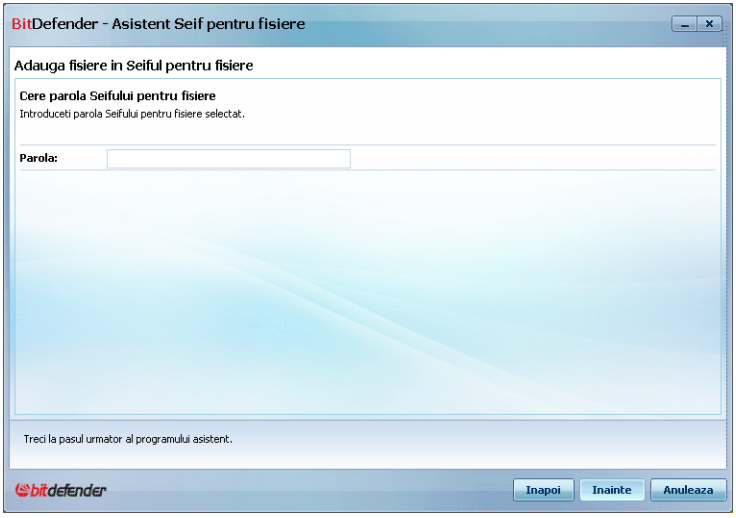
4. Introduceți parola din nou.
5. Setați dimensiunea seifului de fișiere (în MB), tastând un număr în câmpul corespunzător.

Faceți clic pe **Înainte**.

Veți merge la pasul 5.

Pasul 4/6 - Parola

Aici vi se va cere să introduceți parola seifului selectat.

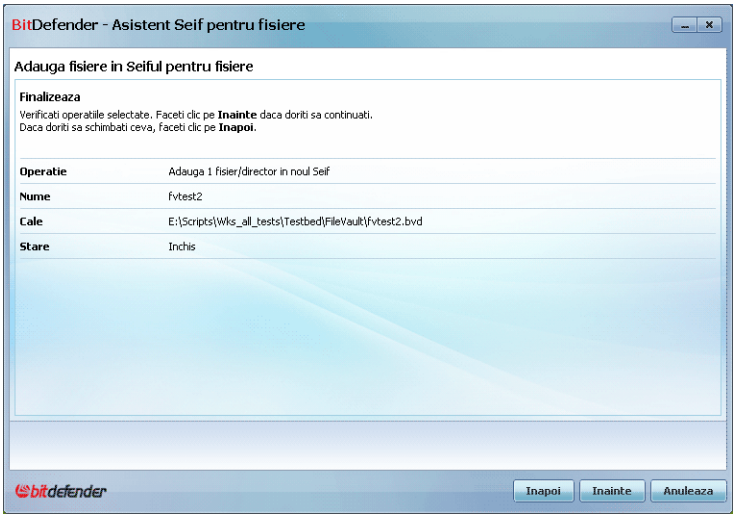


Confirmarea parolei

Introduceți parola în câmpul corespunzător și faceți clic pe **Înainte**.

Step 5/6 - Sumar

Aici puteți vedea operațiile alese.

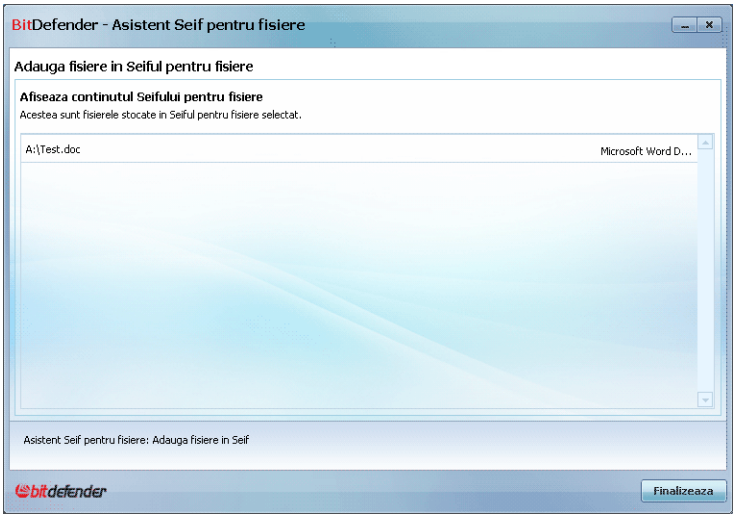


Rezumat

Faceți clic pe **Înainte**.

Pasul 6/6 - Rezultate

Aici puteți vedea conținutul seifului.



Rezultate

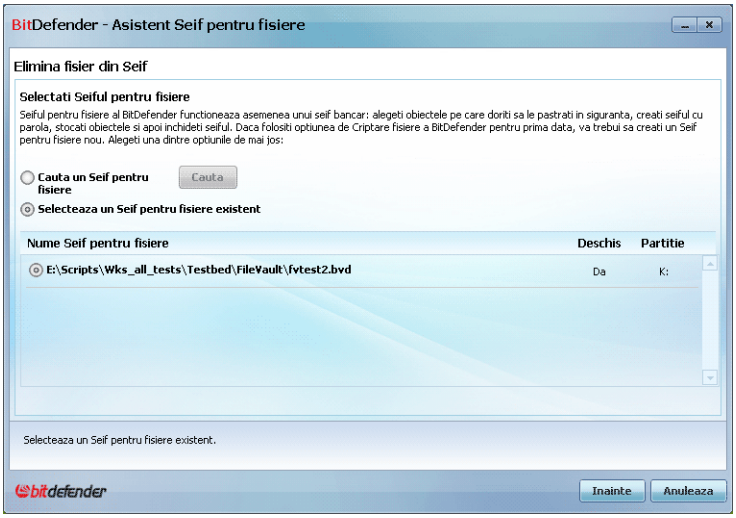
Faceți clic pe **Finalizare**.

11.4.2. Eliminarea fișierelor din seif

Acest program asistent vă ajută să eliminați fișiere dintr-un anumit seif.

Pasul 1/5 - Selectați seiful

Aici puteți specifica seiful din care să ștergeți fișiere.



Selectați seiful

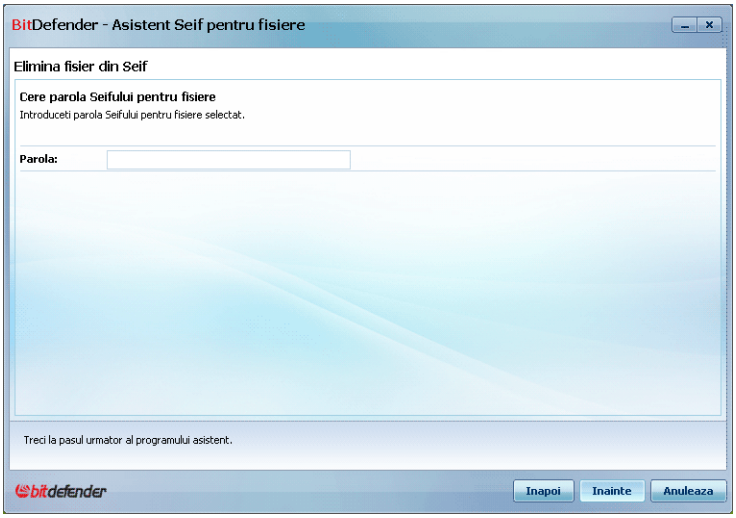
Dacă selectați **Caută un seif de fișiere**, trebuie să faceți clic pe **Caută** și să selectați seiful de fișiere. Veți merge la pasul 3 dacă seiful selectat este deschis sau la pasul 2 dacă este închis.

Dacă faceți clic pe **Selectează un seif de fișiere existent**, trebuie să faceți clic apoi pe numele seifului dorit. Veți merge la pasul 3 dacă seiful selectat este deschis sau la pasul 2 dacă este închis.

Faceți clic pe **Înainte**.

Pasul 2/5 - Parola

Aici vi se va cere să introduceți parola seifului selectat.

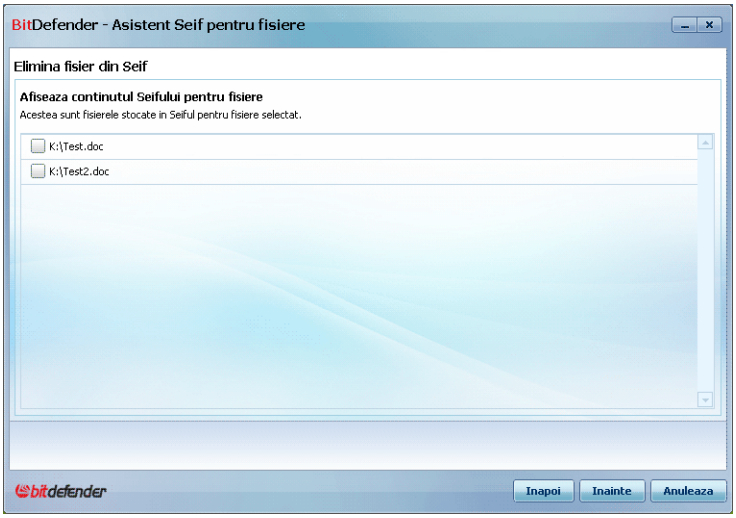


Confirmarea parolei

Introduceți parola în câmpul corespunzător și faceți clic pe **Înainte**.

Pasul 3/5 - Selectați fișierele

Aici vor fi afișate fișierele din seiful selectat anterior.

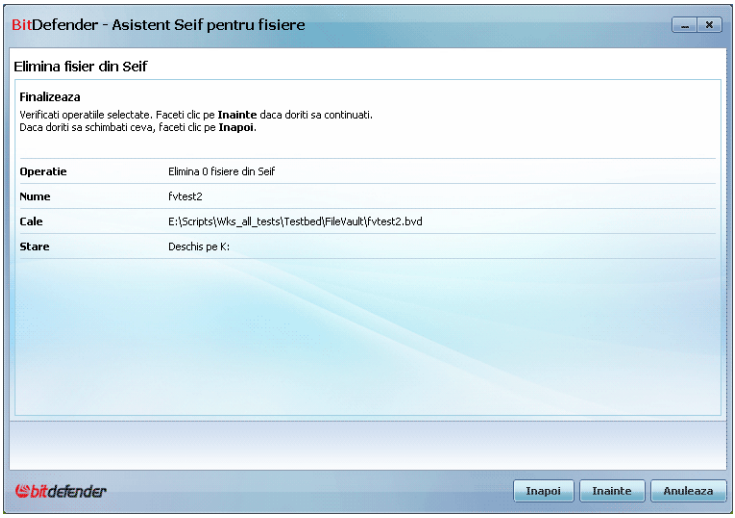


Selectați fișierele

Selectați fișierele care să fie șterse și faceți clic pe **Înainte**.

Pasul 4/5 - Rezumat

Aici puteți vedea operațiile alese.

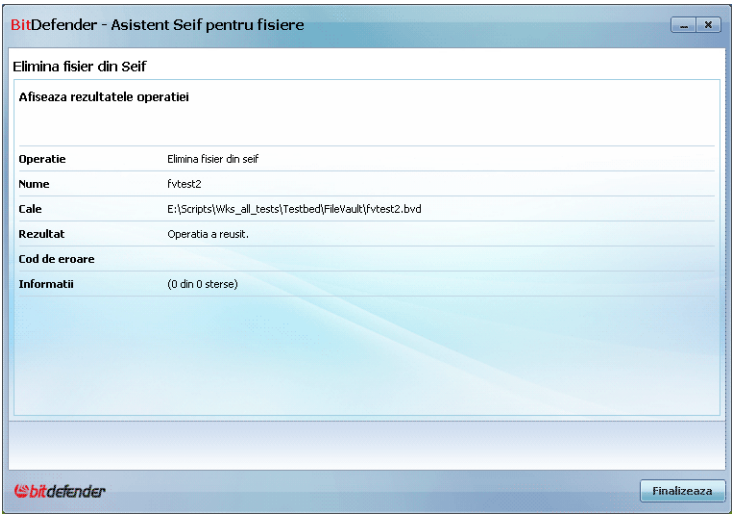


Rezumat

Faceți clic pe **Înainte**.

Pasul 5/5 - Rezultate

Aici puteți vedea rezultatul operației.



Rezultate

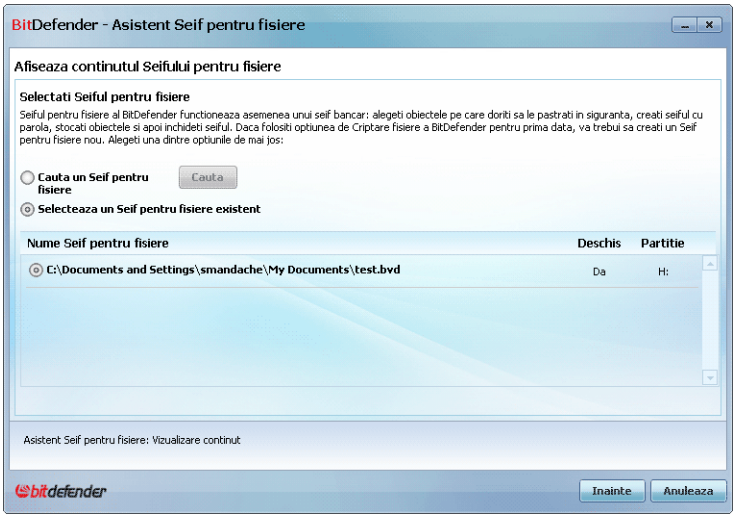
Faceți clic pe **Finalizare**.

11.4.3. Vizualizarea Seifului pentru fișiere

Acest program asistent vă ajută să deschideți un anumit seif pentru fișiere și să vizualizați fișierele pe care le conține acesta.

Pasul 1/4 - Selectați seiful

Aici puteți specifica seiful ale cărui fișiere doriți să le vedeți.



Selectați seiful

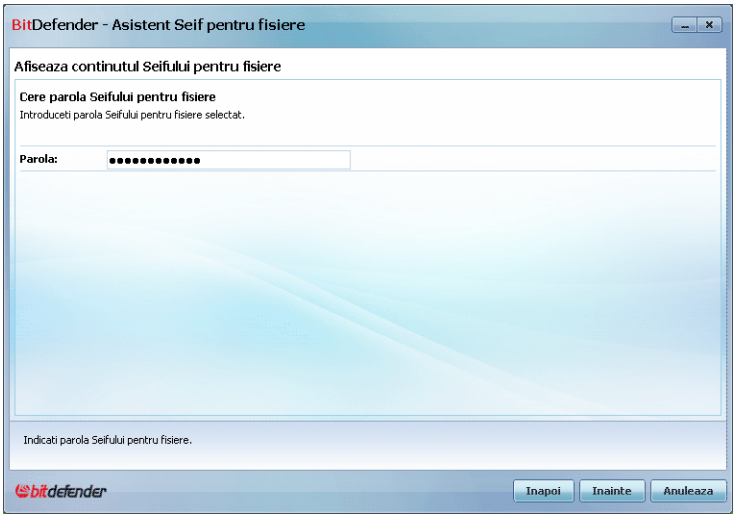
Dacă selectați **Caută un seif de fișiere**, trebuie să faceți clic pe **Caută** și să selectați seiful de fișiere. Veți merge la pasul 3 dacă seiful selectat este deschis sau la pasul 2 dacă este închis.

Dacă faceți clic pe **Selectează un seif de fișiere existent**, trebuie să faceți clic apoi pe numele seifului dorit. Veți merge la pasul 3 dacă seiful selectat este deschis sau la pasul 2 dacă este închis.

Faceți clic pe **Înainte**.

Pasul 2/4 - Parola

Aici vi se va cere să introduceți parola seifului selectat.

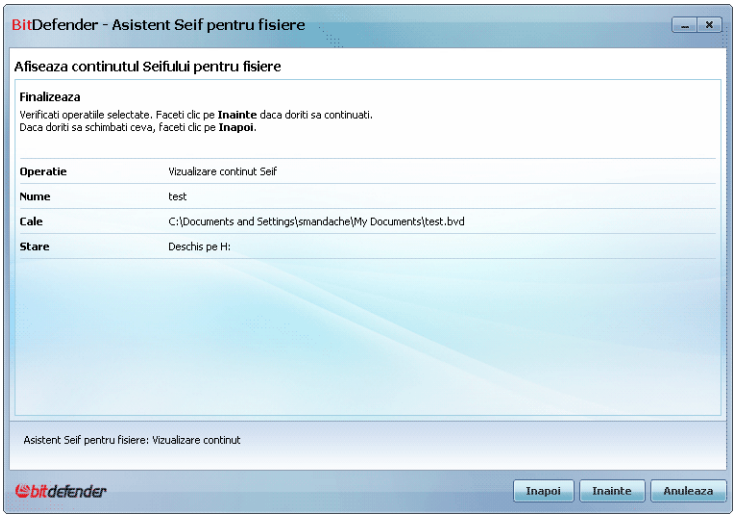


Confirmarea parolei

Introduceți parola în câmpul corespunzător și faceți clic pe **Înainte**.

Pasul 3/4 - Rezumat

Aici puteți vedea operațiile alese.

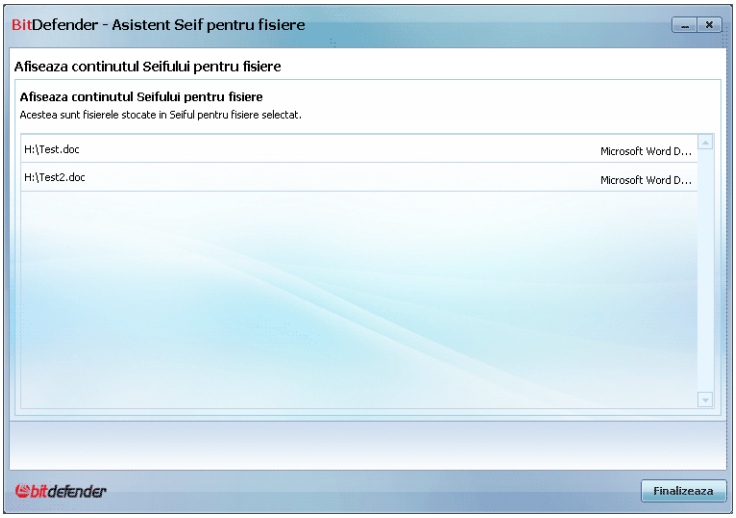


Rezumat

Faceți clic pe **Înainte**.

Pasul 4/4 - Rezultate

Aici puteți vedea fișierele din seif.



Rezultate

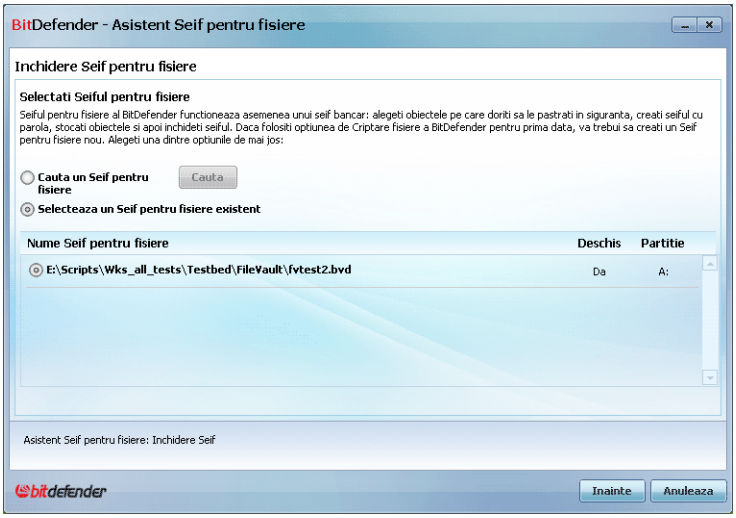
Faceți clic pe **Finalizare**.

11.4.4. Închiderea Seifului pentru fișiere

Acest program asistent vă ajută să închideți un anumit seif pentru fișiere pentru a proteja fișierele pe care le conține acesta.

Pasul 1/3 - Selectați seiful

Aici puteți specifica seiful care să fie închis.



Selectați seiful

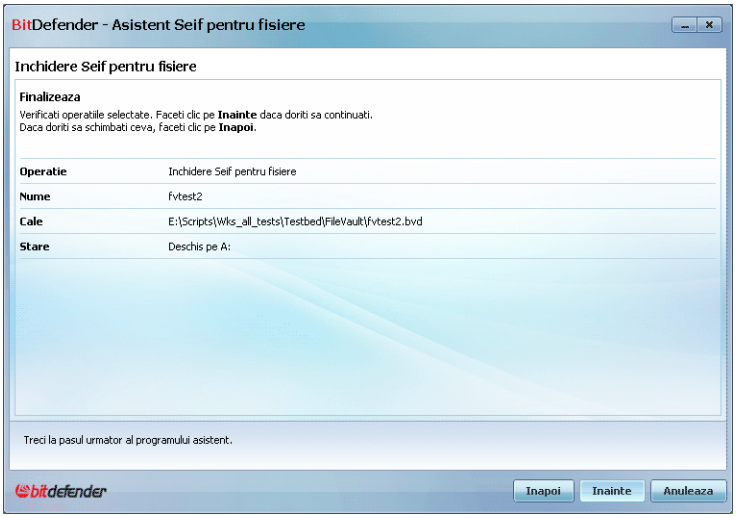
Dacă selectați **Caută un seif de fișiere**, trebuie să faceți clic pe **Caută** și să selectați seiful de fișiere.

Dacă faceți clic pe **Selectează un seif de fișiere existent**, trebuie să faceți clic apoi pe numele seifului dorit.

Faceți clic pe **Înainte**.

Pasul 2/3 - Rezumat

Aici puteți vedea operațiile alese.

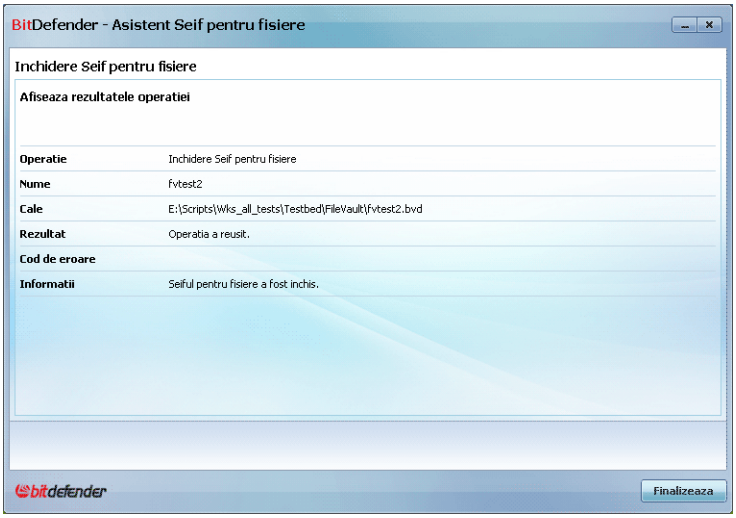


Rezumat

Faceți clic pe **Înainte**.

Pasul 3/3 - Rezultate

Aici puteți vedea rezultatul operației.



Rezultate

Faceți clic pe **Finalizare**.

Modul Intermediar

12. Pagina de stare

Tabul Pagina de Stare oferă informații legate de starea de securitate a calculatorului dvs și vă permite să remediați problemele în așteptare.

Pagina de stare

Pagina de stare conține următoarele secțiuni:

- **Stare generală** - Arată câte probleme afectează securitatea calculatorului dumneavoastră și vă ajută să le rezolvați. Dacă există probleme în așteptare, veți vedea un **cerc roșu cu semnul exclamării** și butonul **Remediază**. Faceți clic pe buton pentru a porni asistentul Remediază probleme.
- **Detalii stare** - Indică starea fiecărui modul principal folosind propoziții explicite și una dintre următoarele iconițe:

  Cerc verde cu bifă: Nicio problemă de securitate. Calculatorul și datele dvs sunt protejate.

  Cerc gri cu semnul exclamării: Activitatea componentelor acestui modul nu este monitorizată. Prin urmare, nu sunt disponibile informații legate de starea lor de securitate. Pot exista anumite probleme legate de acest modul.

  Cerc roșu cu semnul exclamării: Mai multe probleme afectează securitatea sistemului dumneavoastră. Problemele majore necesită atenția dvs imediat. Problemele minore trebuie remediate cât mai curând.

Faceți clic pe numele unui modul pentru a vedea mai multe detalii despre starea sa și pentru a configura monitorizarea stării componentelor sale.

- **Profil utilizator** - Indică profilul de utilizator selectat în acel moment și oferă un link către o sarcină relevantă pentru acesta:
  - La selectarea profilului **Tipic**, butonul **Scanează acum** vă permite să efectuați o Scanare de sistem folosind Asistentul de Scanare antivirus. Va fi scanat întregul sistem, cu excepția arhivelor. În configurația implicită, se scanează după toate tipurile de aplicații periculoase, altele decât cele de tip rootkit.
  - Dacă este selectat profilul **Părinte**, butonul **Control parental** vă permite să configurați setările de Control parental. Pentru informații more referitoare la configurarea Controlului parental, consultați capitolul *„Control parental”* (p. 189).
  - La selectarea profilului **Jucător**, butonul **Pornește/oprește Modul pentru jocuri** vă permite să activați/dezactivați Modul pentru jocuri. Modul pentru jocuri modifică temporar setările produsului pentru a minimiza impactul acestora asupra performanței sistemului.
  - La selectarea profilului **Personal**, butonul **Actualizează acum** pornește imediat actualizarea. Va apărea o nouă fereastră în care puteți vedea starea actualizării.

  Dacă doriți să treceți la un alt profil sau să-l editați pe care îl folosiți, faceți clic pe profil și urmați asistentul de configurare.

13. Securitate

BitDefender conține un modul de securitate care vă ajută să îl actualizați și să vă protejați sistemul de viruși. Pentru a accesa modulul de securitate, faceți clic pe tabul **Securitate**.

Securitate

Modulul Securitate conține două secțiuni:

- **Zona de stare** - Afișează starea curentă a tuturor componentelor de securitate monitorizate și vă permite să alegeți care dintre ele ar trebui să fie monitorizate.
- **Sarcini rapide** - Aici puteți găsi linkuri către cele mai importante sarcini de securitate: actualizare imediată, scanare de sistem, scanare documentele mele, scanare profundă de sistem, scanare personalizată și verificare vulnerabilități.

13.1. Zona de stare

Starea este zona în care puteți vedea lista completă a componentelor de securitate monitorizate și starea lor actuală. Ca urmare a monitorizării fiecărui modul de securitate, BitDefender vă va alerta nu numai când configurați setări care pot afecta securitatea calculatorului dumneavoastră, ci și atunci când uitați să executați sarcini importante.

Starea curentă a fiecărei componente este indicată prin propoziții explicite și una dintre următoarele iconițe:

Cerc verde cu bifă: Nicio problemă nu afectează componenta.

Cerc roșu cu semnul exclamării: Mai multe probleme afectează componenta.

Descrierile problemelor apar în roșu. Faceți clic pe butonul **Remediază**din dreptul unei descrieri pentru a remedia problema semnalată. Dacă o problemă nu este remediată pe loc, urmați pașii programului asistent.

13.1.1. Configurarea monitorizării stării

Pentru a selecta componentele pe care BitDefender ar trebui să le monitorizeze, faceți clic pe **Configurare monitorizare stare** și selectați căsuța **Activează alerte** corespunzătoare caracteristicilor care doriți să fie monitorizate.

Important

Este necesar să activați monitorizarea stării componentei dacă doriți să fiți informat despre problemele care afectează securitatea acelei componente. Pentru a vă asigura că sistemul dumneavoastră este complet protejat, activați monitorizarea tuturor componentelor și remediați toate problemele raportate.

Starea următoarelor componente de securitate poate fi monitorizată de BitDefender:

- **Antivirus** - BitDefender monitorizează starea celor două componente ale caracteristicii Antivirus: protecția în timp real și scanarea la cerere. Cele mai frecvente probleme raportate pentru această componentă sunt prezentate în tabelul de mai jos.

Problemă	Descriere
Protecția în timp real este dezactivată	Fișierele nu sunt scanate atunci când sunt accesate de dvs sau de o aplicație care rulează pe acest sistem.
Calculatorul dvs nu a fost scanat niciodată după malware	Nu s-a efectuat nicio scanare de sistem la cerere pentru a se verifica dacă fișierele stocate pe calculatorul dvs nu sunt infectate.
Ultima scanare de sistem pe care ați început-o a fost anulată înainte de finalizare	S-a pornit dar nu s-a finalizat o scanare completă de sistem.
Antivirus în stare critică	Protecția în timp real este dezactivată și sistemul nu a fost scanat de mult timp.

- **Actualizare** - BitDefender monitorizează dacă semnăturile aplicațiilor periculoase sunt actualizate. Cele mai frecvente probleme raportate pentru această componentă sunt prezentate în tabelul de mai jos.

Problemă	Descriere
Actualizarea automată este dezactivată	Semnăturile aplicațiilor periculoase din baza de date a produsului dvs BitDefender nu sunt actualizate automat, în mod regulat.
Actualizarea nu a mai fost efectuată de x zile	Semnăturile aplicațiilor periculoase din baza de date a produsului dvs BitDefender nu sunt actualizate.

- **Firewall** - BitDefender monitorizează starea Firewallului. Dacă acesta nu este activat, se va raporta problema **Firewall dezactivat**.
- **Antispam** - BitDefender monitorizează starea caracteristicii Antispam. Dacă aceasta nu este activată, se va raporta problema **Antispam dezactivat**.
- **Antiphishing** - BitDefender monitorizează starea modulului Antiphishing. Dacă nu este activat pentru toate aplicațiile admise, se va raporta problema **Antiphishing dezactivat**.
- **Verificare vulnerabilități** - BitDefender monitorizează caracteristica verificare vulnerabilități. Aceasta vă permite să aflați dacă e necesar să instalați actualizări Windows, ale aplicațiilor sau dacă e nevoie să modificați o parolă vulnerabilă.

  Cele mai frecvente probleme raportate pentru această componentă sunt prezentate în tabelul de mai jos.

Stare	Descriere
Verificare vulnerabilități dezactivată	BitDefender nu verifică dacă există vulnerabilități legate de actualizări Windows lipsă, aplicarea actualizărilor sau stabilirea unor parole simple.
S-au detectat mai multe vulnerabilități	BitDefender a identificat actualizări Windows/ale aplicațiilor lipsă și/sau parole vulnerabile.
Actualizări Microsoft critice	Actualizări Microsoft esențiale sunt disponibile, dar nu sunt instalate.
Alte actualizări Microsoft	Actualizări Microsoft obișnuite sunt disponibile, dar nu sunt instalate.
Actualizare automată Windows dezactivată	Actualizările de securitate Windows nu sunt instalate automat imediat ce devin disponibile.
`Aplicație` (neactualizată)	O nouă versiune a `Aplicației` este disponibilă, dar nu este instalată.
`Utilizator` (Parolă vulnerabilă)	O parolă a utilizatorului este ușor de identificat de persoane periculoase, care folosesc programe specializate.

13.2. Sarcini rapide

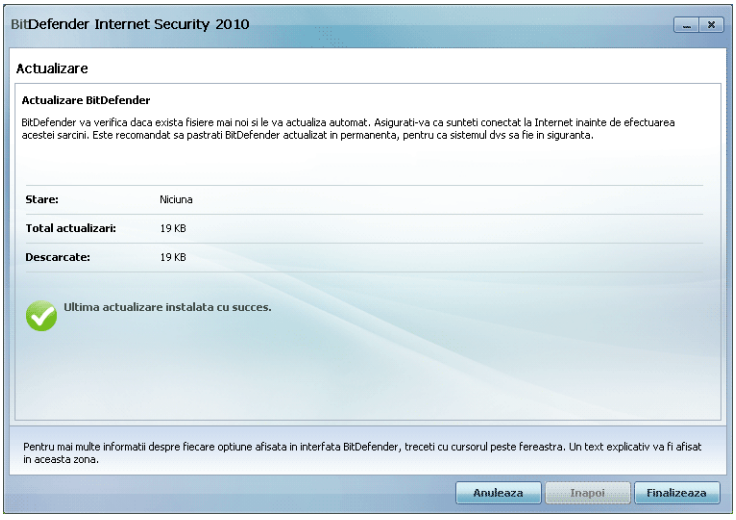
Aici găsiți linkuri către cele mai importante sarcini de securitate:

- **Actualizează acum** - inițiază o actualizare imediată.
- **Scanare de sistem** - pornește o scanare standard a întregului calculator (fără arhive). Pentru sarcini de scanare la cerere suplimentare, faceți clic pe săgeata de pe acest buton și selectați o altă sarcină de scanare: Scanare Documentele mele sau Scanare profundă de sistem.
- **Scanare personalizată** - pornește un asistent care vă permite să creați și să rulați o sarcină de scanare personalizată.
- **Scanare vulnerabilități** - pornește programul asistent care verifică sistemul de vulnerabilități și vă ajută să le rezolvați.

13.2.1. Actualizarea BitDefender

În fiecare zi sunt descoperite și identificate noi aplicații malițioase. De aceea, este foarte importantă actualizarea BitDefender cu ultimele semnături de aplicații malițioase.

În mod implicit, BitDefender caută actualizări atunci când deschideți calculatorul și apoi **la fiecare oră**. Cu toate acestea, dacă doriți să actualizați BitDefender, trebuie doar să faceți clic pe **Actualizează acum**. Procesul de actualizare va fi inițiat și următoarea fereastră va apărea imediat:



Actualizarea BitDefender

În această fereastră puteți vedea stadiul procesului de actualizare.

Procesul de actualizare este realizat progresiv, ceea ce inseamna ca fisierele care trebuie actualizate sunt inlocuite unul cate unul. Astfel, procesul de actualizare nu va afecta funcționarea produsului și, în același timp, orice vulnerabilitate va fi exclusă.

Dacă doriți să închideți această fereastră, faceți clic pe **Anulare**. Aceasta nu va opri procesul de actualizare.

Notă
Dacă vă conectați la Internet prin dial-up, atunci este recomandat să actualizați manual BitDefender în mod regulat.

Reporniți calculatorul, dacă este necesar. În cazul unei actualizari majore, vi se va cere să reporniți calculatorul. Faceți clic pe **Reboot** pentru a vă reporni imediat sistemul.

Dacă doriți să reporniți calculatorul mai târziu,, faceți clic pe **OK**. Vă recomandăm să reporniți calculatorul cât mai curând posibil.

13.2.2. Scanarea cu BitDefender

Pentru a vă scana calculatorul după malware, rulați o sarcină de scanare facând clic pe butonul corespunzător sau selectând-o din meniul derulabil. Tabelul următor prezintă sarcinile de scanare disponibile, împreună cu descrierea lor:

Sarcina	Descriere
Scanare de sistem	Scanează întregul sistem, cu excepția arhivelor. În configurația implicită, scanează după toate tipurile de aplicații periculoase, altele decât cele de tip rootkit.
Scanează documente	Utilizați această sarcină pentru a scana directoare importante ale utilizatorului curent: `My Documents`, `Desktop` și `StartUp`. Astfel, veți asigura siguranța documentelor dumneavostră, un spațiu de lucru sigur și rularea la pornirea sistemului a unor aplicații necompromise.
Scanare profundă sistem	Scanează întregul sistem. În configurația implicită, se scanează după toate tipurile de aplicații malițioase care amenință securitatea sistemului dumneavoastră, cum ar fi virușii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) și altele.
Scanare personalizată	Utilizați această sarcină pentru a selecta direct care fișiere și directoare să fie scanate.

Notă

Deoarece sarcinile **Scanare profundă sistem** și **Scanare completă sistem** analizează întregul sistem, procesul poate fi unul de durată. De aceea, vă recomandăm să rulați aceste sarcini cu prioritate scăzută sau chiar atunci când nu utilizați calculatorul.

Când rulați o sarcină de Scanare de sistem, Scanare profundă de sistem sau Scanare Documentele mele, va apărea un asistent de Scanare Antivirus. Urmați programul asistent în trei pași pentru a realiza procesul de scanare. Pentru informații detaliate despre acest program asistent, consultați secțiunea *„Programul asistent de scanare”* (p. 57).

Când rulați o Scanare personalizată, Asistentul de Scanare personalizată vă va ghida de-a lungul procesului. Urmați procedura în șase pași pentru a scana anumite fișiere sau directoare. Pentru informații detaliate despre acest program asistent, consultați secțiunea *„Asistent scanare personalizată”* (p. 61).

13.2.3. Verificare vulnerabilități

Programul asistent de căutare a vulnerabilităților verifică sistemul de actualizare al Microsoft Windows și al Microsoft Windows Office și parolele conturilor Microsoft Windows pentru a vă asigura că sistemul dumneavoastră de operare este actualizat și că parolele nu pot fi ghicite ușor.

Pentru a verifica dacă sistemul dvs este vulnerabil, faceți clic pe **Scanare vulnerabilități** și urmați programului asistent în șase pași. Pentru mai multe informații, consultați capitolul *„Remedierea vulnerabilităților”* (p. 244).

14. Parental

BitDefender Internet Security 2010 include un modul de control parental. Controlul parental vă permite să restricționați accesul copiilor la Internet și la anumite aplicații. Pentru a verifica starea Controlului parental, faceți clic pe tabul **Parental**.

Parental

Modulul Parental conține două secțiuni:

- **Zonă stare** - Vă permite să vedeți dacă modulul Control parental este configurat și să activați/dezactivați monitorizarea activității acestuia.
- **Sarcini rapide** - Aici puteți găsi linkuri către cele mai importante sarcini de securitate: scanare de sistem, scanare profundă, actualizare imediată.

14.1. Zona de stare

Starea curentă a modulului Control Parental este indicată prin propoziții explicite și una dintre următoarele iconițe:

Cerc verde cu bifă: Nicio problemă nu afectează componenta.

Cerc roșu cu semnul exclamării: Mai multe probleme afectează componenta.

Descrierile problemelor apar în roșu. Faceți clic pe butonul **Remediază**din dreptul unei descrieri pentru a remedia problema semnalată. Problema cea mai frecvent raportată pentru acest modul este **Control parental neconfigurat**.

Dcaă doriți ca BitDefender să monitorizeze modulul Control parental, faceți clic pe **Configurare monitorizare stare** și selectați căsuța **Activează alerte** corespunzătoare acestui modul.

14.2. Sarcini rapide

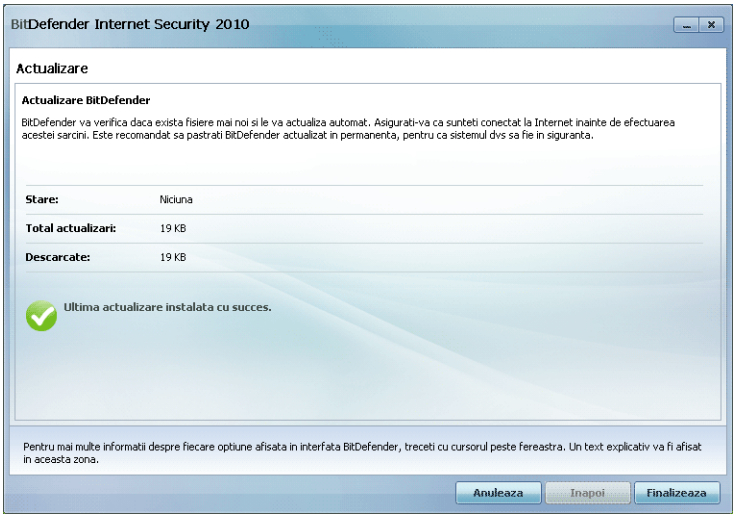
Aici găsiți linkuri către cele mai importante sarcini de securitate:

- **Actualizează acum** - inițiază o actualizare imediată.
- **Scanare de sistem** - inițiază o scanare completă a calculatorului dumneavoastră (arhivele nu sunt scanate).
- **Scanare profundă sistem** - inițiază o scanare completă a calculatorului dumneavoastră (inclusiv arhivele).

14.2.1. Actualizarea BitDefender

În fiecare zi sunt descoperite și identificate noi aplicații malițioase. De aceea, este foarte importantă actualizarea BitDefender cu ultimele semnături de aplicații malițioase.

În mod implicit, BitDefender caută actualizări atunci când deschideți calculatorul și apoi **la fiecare oră**. Cu toate acestea, dacă doriți să actualizați BitDefender, trebuie doar să faceți clic pe **Actualizează acum**. Procesul de actualizare va fi inițiat și următoarea fereastră va apărea imediat:



Actualizarea BitDefender

În această fereastră puteți vedea stadiul procesului de actualizare.

Procesul de actualizare este realizat progresiv, ceea ce inseamna ca fisierele care trebuie actualizate sunt inlocuite unul cate unul. Astfel, procesul de actualizare nu va afecta funcționarea produsului și, în același timp, orice vulnerabilitate va fi exclusă.

Dacă doriți să închideți această fereastră, faceți clic pe **Anulare**. Aceasta nu va opri procesul de actualizare.

Notă
Dacă vă conectați la Internet prin dial-up, atunci este recomandat să actualizați manual BitDefender în mod regulat.

Reporniți calculatorul, dacă este necesar. În cazul unei actualizari majore, vi se va cere să reporniți calculatorul. Faceți clic pe **Reboot** pentru a vă reporni imediat sistemul.

Dacă doriți să reporniți calculatorul mai târziu,, faceți clic pe **OK**. Vă recomandăm să reporniți calculatorul cât mai curând posibil.

14.2.2. Scanarea cu BitDefender

Pentru a vă scana calculatorul după malware, rulați o sarcină de scanare facând clic pe butonul corespunzător. Tabelul următor prezintă sarcinile de scanare disponibile, împreună cu descrierea lor:

Sarcina	Descriere
Scanare de sistem	Scanează întregul sistem, cu excepția arhivelor. În configurația implicită, scanează după toate tipurile de aplicații periculoase, altele decât cele de tip rootkit.
Scanare profundă sistem	Scanează întregul sistem. În configurația implicită, se scanează după toate tipurile de aplicații malițioase care amenință securitatea sistemului dumneavoastră, cum ar fi virușii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) și altele.

Notă
Deoarece sarcinile **Scanare profundă sistem** și **Scanare completă sistem** analizează întregul sistem, scanarea poate lua ceva timp. De aceea, vă recomandăm să rulați aceste sarcini cu prioritate scăzută sau, și mai bine, atunci când nu utilizați calculatorul.

Când executați o scanare, va apărea programul asistent de scanare. Urmați programul asistent în trei pași pentru a realiza procesul de scanare. Pentru informații

detaliate despre acest program asistent, consultați secțiunea *„Programul asistent de scanare”* (p. 57).

15. Seif de fișiere

BitDefender include un modul Seif pentru fișiere care vă ajută să păstrați în siguranță datelor dvs confidențiale. Pentru aceasta, folosiți opțiunea de criptare a fișierelor.

Cu ajutorul acestei caracteristici, puteți proteja fișierele prin plasarea lor în seifuri pentru fișiere.

- Seiful de fișiere reprezintă un spațiu sigur de stocare a informațiilor personale sau a fișierelor confidențiale.
- Seiful de fișiere este de fapt un fișier criptat de pe calculatorul dumneavoastră, având extensia bvd. Seiful de fișiere fiind criptat, datele dinăuntrul acestuia sunt protejate împotriva furtului sau a altor pericole informatice.
- Atunci când deschideți acest fișier bvd, va apărea o nouă partiție logică (un nou drive). Veți întelege mai ușor procesul prin analogie cu un proces similar: montarea unei imagini ISO ca CD virtual.

  Deschideți My Computer și veți vedea un nou drive, care corespunde seifului dumneavoastră de fișiere. Puteți face diverse operații cu fișierele din seif (copiere, ștergere, modificare etc). Fișierele sunt protejate cât timp se află în acest drive (deoarece este nevoie de parolă pentru deschiderea acestuia).

  Atunci când ați terminat ce aveați de făcut, închideți seiful pentru a proteja conținutul acestuia.

Pentru a accesa modulul Seif fișiere, faceți clic pe tabul **Seif fișiere**.

Seif de fișiere

Modulul Seif fișiere conține două secțiuni:

- **Zonă stare** - Vă permite să vedeți lista completă a componentelor monitorizate. Puteți alege care dintre componente să fie monitorizate. Este recomandată monitorizarea tuturor componentelor.
- **Sarcini rapide** - Aici puteți găsi linkuri către cele mai importante sarcini de securitate: adăugare, vizualizare, închidere și ștergere seifuri pentru fișiere.

15.1. Zona de stare

Starea curentă a fiecărei componente este indicată prin propoziții explicite și una dintre următoarele iconițe:

Cerc verde cu bifă: Nicio problemă nu afectează componenta.

Cerc roșu cu semnul exclamării: Mai multe probleme afectează componenta.

Descrierile problemelor apar în roșu. Faceți clic pe butonul **Remediază**din dreptul unei descrieri pentru a remedia problema semnalată. Dacă o problemă nu este remediată pe loc, urmați pașii programului asistent.

Zona de stare din tabul Seif pentru fișiere oferă informații despre starea modulului **Criptare fișiere**.

Dcaă doriți ca BitDefender să monitorizeze opțiunea Criptare fișiere, faceți clic pe **Configurare monitorizare stare** și selectați căsuța **Activează alerte**.

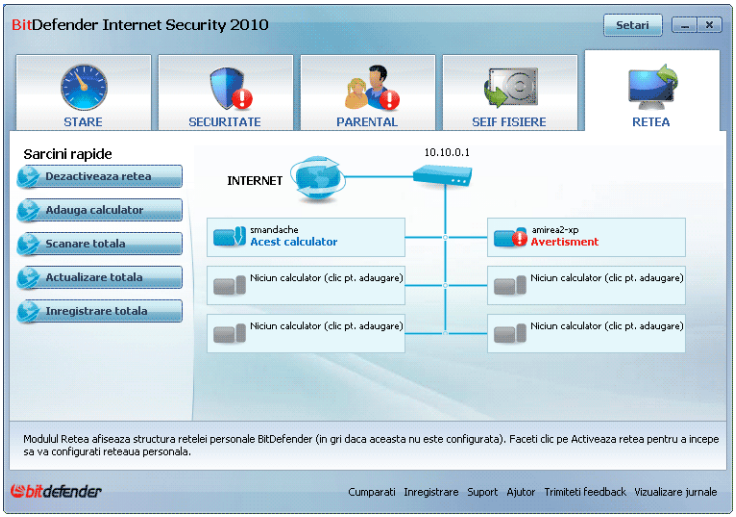
15.2. Sarcini rapide

Următoarele butoane sunt disponibile:

- **Adaugă fișier în seif** - pornește programul asistent care vă permite să stocați în siguranță fișierele / documentele dumneavoastră importante criptându-le în partiții special, securizate (seife de fișiere). Pentru mai multe informații, consultați capitolul *„Adăugarea fișierelor în seif”* (p. 76).
- **Șterge fișiere din seif** - pornește programul asistent care vă permite să ștergeți date din seiful de fișiere. Pentru mai multe informații, consultați capitolul *„Eliminarea fișierelor din seif”* (p. 82).
- **Vizualizare seif** - pornește programul asistent care vă permite să vedeți conținutul seifurilor dvs pentru fișiere. Pentru mai multe informații, consultați capitolul *„Vizualizarea Seifului pentru fișiere”* (p. 87).
- **Închidere seif** - pornește programul asistent care vă permite să vă închideți seiful, pentru a proteja conținutul acestuia. Pentru mai multe informații, consultați capitolul *„Închiderea Seifului pentru fișiere”* (p. 91).

16. Rețea

Modulul Rețea vă permite să administrați produsele BitDefender instalate pe calculatoarele personale de pe un singur calculator. Pentru a accesa modulul Rețea, faceți clic pe tabul **Rețea**.



Rețea

Pentru a putea administra produsele BitDefender instalate pe calculatoarele personale, trebuie să urmați acești pași:

1. Intrați în rețeaua BitDefender personală de pe calculatorul dumneavoastră. Intrarea în rețea constă în configurarea unei parole administrative pentru modulul Rețea.
2. Mergeți la fiecare calculator pe care doriți să-l administrați și intrați în rețea (setați parola).
3. Întoarceți-vă la calculatorul dumneavoastră și adăugați calculatoarele pe care doriți să le administrați.

16.1. Sarcini rapide

Inițial, un singur buton este disponibil.

- **Activează rețeaua** - vă permite să setați parola rețelei pe care o creați și la care vă conectați.

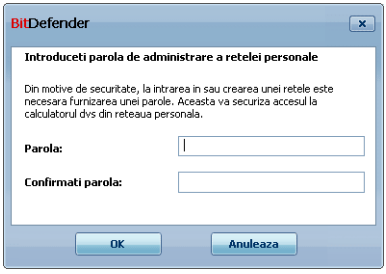
După intrarea în rețea, vor apărea mai multe butoane.

- **Dezactivează rețea** - vă permite să părăsiți rețeaua.
- **Adaugă calculator** - vă permite să adăugați un calculator în rețeaua dumneavoastră.
- **Scanează tot** - vă permite să scanați toate calculatoarele administrate în același timp.
- **Actualizează tot** - vă permite să actualizați toate calculatoarele administrate în același timp.
- **Înregistrează tot** - vă permite să înregistrați toate calculatoarele administrate în același timp.

16.1.1. Intrarea în rețeaua BitDefender

Pentru a în rețeaua BitDefender personală, urmați acești pași:

1. Faceți clic pe **Activare rețea**. Vi se va cere să configurați parola rețelei personale.



Configurare parolă

2. Introduceți aceeași parolă în ambele câmpuri editabile.
3. Faceți clic pe **OK**.

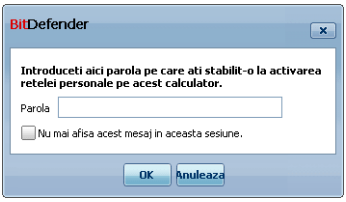
Puteți vedea numele calculatorului apărând pe harta rețelei.

16.1.2. Adăugarea calculatoarelor la rețeaua BitDefender

Înainte de a putea adăuga un calculator la rețeaua BitDefender personală, trebuie să configurați parola rețelei BitDefender pe calculatorul respectiv.

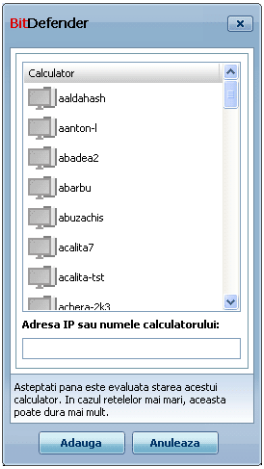
Pentru a adăuga un calculator la rețeaua BitDefender personală, urmați acești pași:

1. Faceți clic pe **Adaugă calculator**. Vi se va cere să furnizați parola locală de administrare a rețelei.



Introducere parolă

2. Introduceți parola de administrare a rețelei și faceți clic pe **OK**. Va apărea o nouă fereastră.



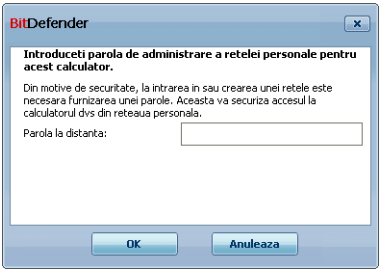
Adaugare calculator

Puteți vedea lista calculatoarelor din rețea. Sensul iconițelor este după cum urmează:

- Indică un calculator online fără niciun produs BitDefender instalat.
- Indică un calculator online cu BitDefender instalat.
- Indică un calculator închis cu BitDefender instalat.

3. Puteți proceda astfel:
   - Selectați din listă numele calculatorului pe care doriți să îl adăugați.
   - Introduceți în câmpul corespunzător adresa IP sau numele calculatorului pe care doriți să îl adăugați.

4. Faceți clic pe **Adaugă**. Vi se va cere să introduceți parola de administrare a rețelei personale configurată pe calculatorul respectiv.



Autentificare

5. Introduceți parola de administrare a rețelei personale configurată pe calculatorul respectiv.
6. Faceți clic pe **OK**. Dacă ați furnizat parola corectă, numele calculatorului selectat va apărea pe harta rețelei.

Notă
Puteți adăuga până la cinci calculatoare pe harta rețelei.

16.1.3. Administrarea rețelei BitDefender

O dată ce ați creat o rețea BitDefender personală, puteți administra toate produsele BitDefender de pe un singur calculator.

Hartă rețea

Dacă plasați cursorul mouse-ului deasupra unui calculator de pe harta rețelei, puteți vedea informații sumare despre acesta (nume, adresă IP, numărul de probleme care afectează securitatea sistemului, starea înregistrării).

Dacă faceți clic-dreapta pe numele unui calculator de pe harta rețelei, puteți vedea toate sarcinile administrative pe care le puteți rula de la distanță pe calculatorul respectiv.

- **Scoate calculatorul din rețeaua personală**

  Vă permite să scoateți un calculator din rețea.

- **Înregistrează BitDefender pe acest calculator**

  Vă permite să înregistrați BitDefender pe acest calculator, prin introducerea unei serii de înregistrare.

- **Stabilește o parola pentru setări pe un calculator la distanță**

  Vă permite să creați o parolă pentru a restricționa accesul la setările BitDefender pe acest calculator.

- **Execută o sarcină de scanare la cerere**

  Vă permite să executați o scanare la cerere pe calculatorul la distanță. Aveți posibilitatea să efectuați oricare din următoarele sarcini de scanare: Scanare My Documents, scanare de sistem sau scanare profundă de sistem.

- **Remediază toate problemele de pe acest calculator**

Vă permite să rezolvați problemele care afectează securitatea acestui calculator, urmând pașii programului asistent Remediază probleme.

- **Vizualizare istoric/evenimente**

  Vă permite să accesați modulul **Istoric&Evenimente** al produsului BitDefender instalat pe acest calculator.

- **Update Now**

  Inițiază procesul de Actualizare a produsului BitDefender instalat pe acest calculator.

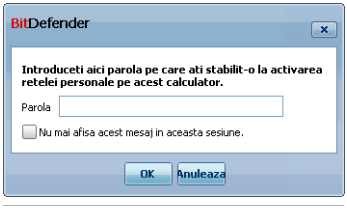
- **Setează profilul de control parental**

  Vă permite să stabiliți categoria de vârstă care va fi folosită de filtrul web al modulului Control Parental pe acest calculator: copil, adolescent sau adult.

- **Stabilește acest calculator ca server de actualizare al acestei rețele**

  Vă permite să setați acest calculator ca server de actualizare pentru toate produsele BitDefender instalate pe calculatoarele din aceasta rețea. Prin folosirea acestei opțiuni, se va reduce traficul pe internet, pentru că numai un calculator din rețea se va conecta la internet pentru a descărca actualizări.

Înainte de a executa o sarcină pe un anumit calculator, vi se va cere să furnizați parola locală de administrare a rețelei.



Introducere parolă

Introduceți parola de administrare a rețelei și faceți clic pe **OK**.

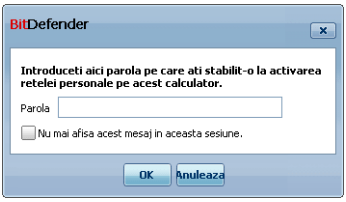
Notă

Dacă doriți să executați mai multe sarcini, puteți selecta **Nu mai afișa mesajul în sesiunea curentă**. Selectând această opțiune, nu vi se va mai cere să introduceți această parolă în sesiunea curentă.

16.1.4. Scanarea tuturor calculatoarelor

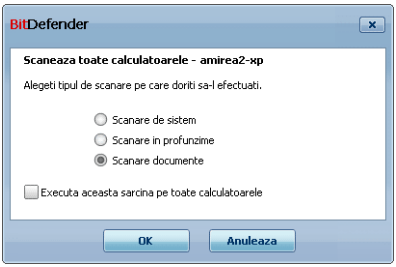
Pentru a scana toate calculatoarele administrate, urmați acești pași:

1. Faceți clic pe **Scanează tot**. Vi se va cere să furnizați parola locală de administrare a rețelei.



Introducere parolă

2. Selectați tipul de analiză.
   - **Scanare de sistem** - inițiază o scanare completă a calculatorului dumneavoastră (arhivele nu sunt scanate).
   - **Scanare profundă sistem** - inițiază o scanare completă a calculatorului dumneavoastră (inclusiv arhivele).
   - **Scanează documente** - inițiază o scanare rapidă a documentelor și setărilor dumneavoastră.



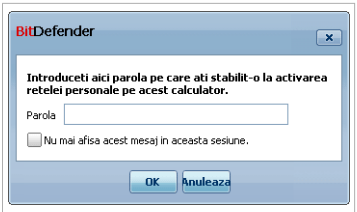
Selectați tipul de analiză.

3. Faceți clic pe **OK**.

16.1.5. Actualizarea tuturor calculatoarelor

Pentru a actualiza toate calculatoarele administrate, urmați acești pași:

1. Faceți clic pe **Actualizează tot**. Vi se va cere să furnizați parola locală de administrare a rețelei.



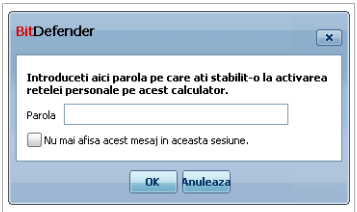
Introducere parolă

2. Faceți clic pe **OK**.

16.1.6. Înregistrarea tuturor calculatoarelor

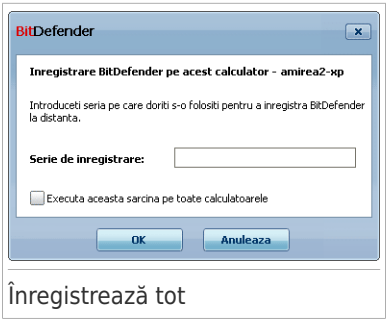
Pentru a înregistra toate calculatoarele administrate, urmați acești pași:

1. Faceți clic pe **Înregistrează tot**. Vi se va cere să furnizați parola locală de administrare a rețelei.



Introducere parolă

2. Introduceți cheia cu care doriți să înregistrați produsele.



Înregistrează tot

3. Faceți clic pe **OK**.

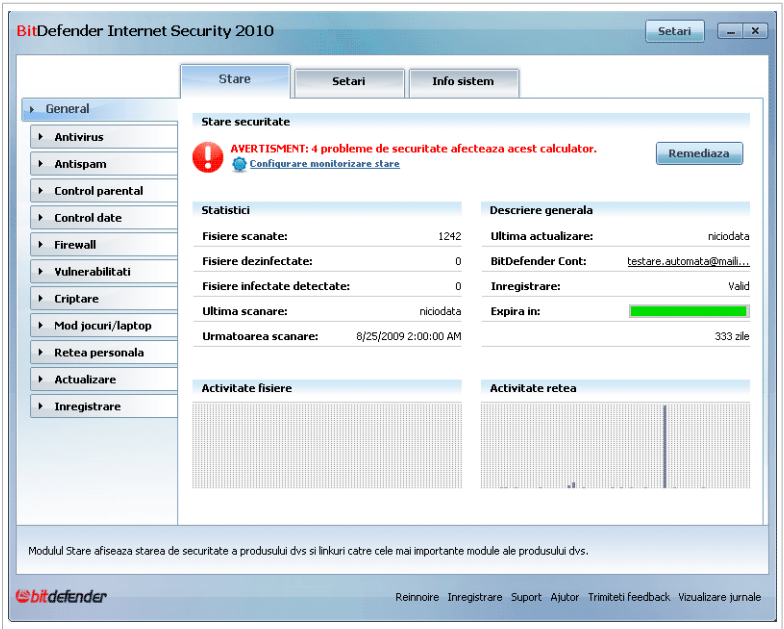
Modul Expert

17. General

Modulul General furnizează informații despre activitatea BitDefender și despre sistem. De asemenea, aici puteți seta comportamentul general al BitDefender.

17.1. Pagina de stare

Pentru a vedea dacă există probleme care afectează calculatorul dvs, precum și statistici legate de activitatea produsului și informații despre stadiul înregistrării, mergeți la **General>Stare** în Modul Expert.



Pagina de stare

Pagina de stare conține mai multe secțiuni:

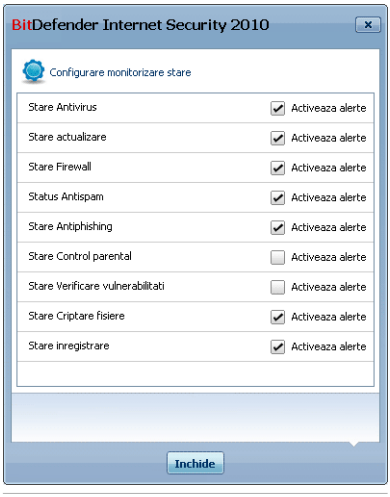
- **Stare generală** - Vă informează despre orice probleme care afectează securitatea calculatorului dvs.
- **Statistici** - Afișează informații importante referitoare la activitatea BitDefender.
- **Prezentare generală** - Afișează informații referitoare la actualizare, contul dumneavoastră, înregistrare și licență.

- **Activitate fișiere** - Indică evoluția numărului de obiecte scanate de către BitDefender Antimalware. Înălțimea barelor indică intensitatea traficului în intervalul de timp respectiv.
- **Activitate rețea** - Indică evoluția traficului din rețea filtrat de Firewallul BitDefender. Înălțimea barelor indică intensitatea traficului în intervalul de timp respectiv.

17.1.1. Stare Generală

Aici puteți afla câte probleme afectează securitatea calculatorului dvs. Pentru a elimina toate amenințările, faceți clic pe **Remediere toate problemele**. Astfel se va lansa asistentul Remediere toate problemele.

Pentru a configura modulele care vor fi monitorizate de BitDefender Internet Security 2010, faceți clic pe **Configurare monitorizare stare** . Va apărea o nouă fereastră:



Configurarea monitorizării stării

Dacă doriți ca BitDefender să monitorizeze o componentă, selectați căsuța **Activează alerte** corespunzătoare acelei componente. Starea următoarelor componente de securitate poate fi monitorizată de BitDefender:

- **Antivirus** - BitDefender monitorizează starea celor două componente ale modulului Antivirus: protecția în timp real și scanarea la cerere. Cele mai frecvente probleme raportate pentru această componentă sunt prezentate în tabelul de mai jos.

Problemă	Descriere
Protecția în timp real este dezactivată	Fișierele nu sunt scanate atunci când sunt accesate de dvs sau de o aplicație care rulează pe acest sistem.
Calculatorul dvs nu a fost scanat niciodată după malware	Nu s-a efectuat nicio scanare de sistem la cerere pentru a se verifica dacă fișierele stocate pe calculatorul dvs nu sunt infectate.
Ultima scanare de sistem pe care ați început-o a fost anulată înainte de finalizare	S-a pornit dar nu s-a finalizat o scanare completă de sistem.
Antivirus în stare critică	Protecția în timp real este dezactivată și sistemul nu a fost scanat de mult timp.

- **Actualizare** - BitDefender monitorizează dacă semnăturile aplicațiilor periculoase sunt actualizate. Cele mai frecvente probleme raportate pentru această componentă sunt prezentate în tabelul de mai jos.

Problemă	Descriere
Actualizarea automată este dezactivată	Semnăturile aplicațiilor periculoase din baza de date a produsului dvs BitDefender nu sunt actualizate automat, în mod regulat.
Actualizarea nu a mai fost efectuată de x zile	Semnăturile aplicațiilor periculoase din baza de date a produsului dvs BitDefender nu sunt actualizate.

- **Firewall** - BitDefender monitorizează starea Firewallului. Dacă acesta nu este activat, se va raporta problema **Firewall dezactivat**.
- **Antispam** - BitDefender monitorizează starea caracteristicii Antispam. Dacă aceasta nu este activată, se va raporta problema **Antispam dezactivat**.
- **Antiphishing** - BitDefender monitorizează starea modulului Antiphishing. Dacă nu este activat pentru toate aplicațiile admise, se va raporta problema **Antiphishing dezactivat**.
- **Control parental** - BitDefender monitorizează starea caracteristicii Control parental. Dacă aceasta nu este activată, se va raporta problema **Control parental neconfigurat**.
- **Verificare vulnerabilități** - BitDefender monitorizează caracteristica verificare vulnerabilități. Aceasta vă permite să aflați dacă e necesar să instalați actualizări Windows, ale aplicațiilor sau dacă e nevoie să modificați o parolă vulnerabilă.

Cele mai frecvente probleme raportate pentru această componentă sunt prezentate în tabelul de mai jos.

Stare	Descriere
Verificare vulnerabilități dezactivată	BitDefender nu verifică dacă există vulnerabilități legate de actualizări Windows lipsă, aplicarea actualizărilor sau stabilirea unor parole simple.
S-au detectat mai multe vulnerabilități	BitDefender a identificat actualizări Windows/ale aplicațiilor lipsă și/sau parole vulnerabile.
Actualizări Microsoft critice	Actualizări Microsoft esențiale sunt disponibile, dar nu sunt instalate.
Alte actualizări Microsoft	Actualizări Microsoft obișnuite sunt disponibile, dar nu sunt instalate.
Actualizare automată Windows dezactivată	Actualizările de securitate Windows nu sunt instalate automat imediat ce devin disponibile.
Aplicație (neactualizată)	O nouă versiune a `Aplicației` este disponibilă, dar nu este instalată.
Utilizator (Parolă vulnerabilă)	O parolă a utilizatorului este ușor de identificat de persoane periculoase, care folosesc programe specializate.

- **Criptare fișiere** - BitDefender monitorizează starea caracteristicii Criptare fișiere. Dacă aceasta nu este activată, se va raporta problema **Criptare fișiere dezactivată**.

Important
Pentru a vă asigura că sistemul dumneavoastră este complet protejat, activați monitorizarea tuturor componentelor și remediați toate problemele raportate.

17.1.2. Statistici

Dacă doriți să urmăriți activitatea BitDefender, puteți începe cu secțiunea Statistici. Următoarele elemente sunt afișate:

Element	Descriere
Fișiere scanate	Indică numărul de fișiere care au fost verificate după malware la ultima scanare.
Fișiere dezinfectate	Indică numărul de fișiere care au fost dezinfectate la ultima scanare.

Element	Descriere
Fisiere infectate detectate	Indică numărul de fișiere infectate detectate în sistemul dumneavoastră la ultima scanare.
Ultima scanare de sistem	Arată când a fost scanat ultima oară calculatorul dumneavoastră. Dacă ultima scanare a fost efectuată cu mai mult de o săptămână în urmă, scanați calculatorul cât mai repede posibil. Pentru a scana tot calculatorul, mergeți la **Antivirus**, tabul Scanare virusi și rulați una dintre aceste sarcini: Scanare profundă sistem sau Scanare completă sistem.
Următoarea scanare	Arată când urmează să fie scanat calculatorul dumneavoastră.

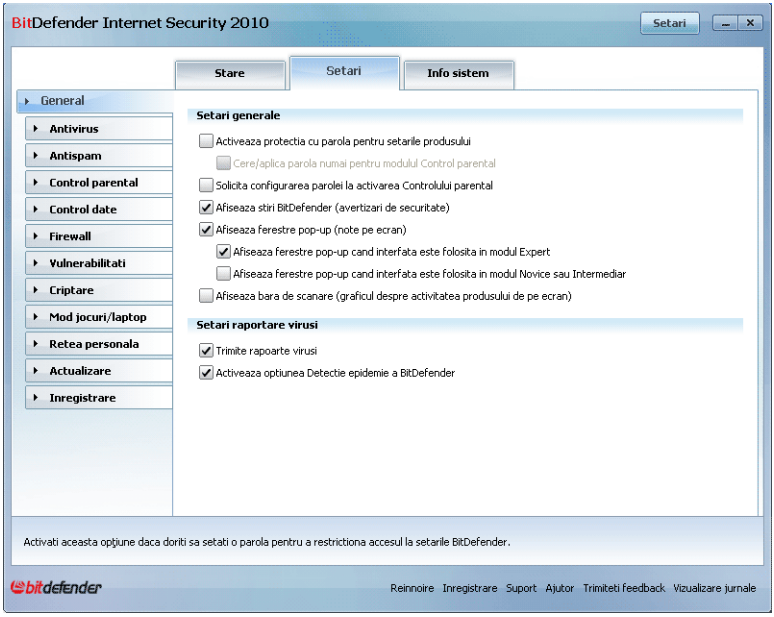
17.1.3. Descriere generală

Aici puteți vedea informații cu privire la actualizare, contul dumneavoastră, înregistrare și licență.

Element	Descriere
Ultima actualizare	Arată când a fost actualizat ultima oară produsul dumneavoastră BitDefender. Vă rugăm să efectuați actualizări în mod regulat, pentru a avea un sistem complet protejat.
Cont BitDefender	Indică adresa de e-mail pe care o puteți utiliza pentru a vă accesa contul online, unde vă puteți recupera seria de înregistrare pierdută și puteți beneficia de suport BitDefender si alte servicii personalizate. Trebuie să creați un cont BitDefender pentru a activa produsul. Pentru a afla informații despre contul BitDefender, consultați secțiunea *„Înregistrare și Contul meu”* (p. 52).
Înregistrare	Indică tipul și starea seriei dumneavoastră de înregistrare. Pentru a menține securitatea sistemului dumneavoastră, trebuie să reînnoiți sau să actualizați versiunea BitDefender în cazul în care seria dumneavoastră a expirat.
Expiră în	Indică numărul de zile rămase până la expirarea seriei de înregistrare. Dacă seria dumneavoastră de înregistrare expiră în următoarele zile, vă rugăm să înregistrați produsul cu o nouă serie de înregistrare. Pentru a achiziționa o serie de înregistrare sau pentru a vă reînnoi licența, faceți clic pe linkul **Cumpără**, situat în partea de jos a ferestrei.

17.2. Setări

Pentru a configura și administra setările generale ale BitDefender, faceți clic pe **General>Setări** în Modul Expert.



Setări generale

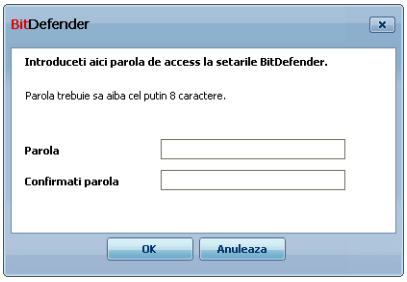
Aici puteți seta comportamentul general al produsului. BitDefender se încarcă la pornirea Windows iar apoi rulează minimizat în bara de sistem.

17.2.1. Setări generale

- **Activează protecția prin parolă pentru setările produsului** - permite setarea unei parole pentru a proteja configurația BitDefender.

  Notă
  Dacă nu sunteți singura persoană cu drepturi administrative care folosește acest calculator, este recomandat să vă protejați setările BitDefender cu o parolă.

  Dacă selectați această opțiune, va apărea următoarea fereastră:



Confirmarea parolei

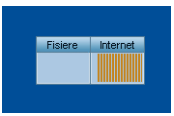
Introduceți parola în câmpul **Parolă**, reintroduceți-o în câmpul **Reintroduceți parola** și faceți clic pe **OK**.

După ce ați setat parola, vi se va cere să o introduceți ori de câte ori doriți să modificați setările BitDefender. De asemenea, ceilalți administratori de sistem (dacă există) vor trebui să furnizeze această parolă pentru a schimba setările BitDefender.

Dacă doriți să fie cerută parola doar la configurarea controlului parental, trebuie să selectați și opțiunea **Cere/Aplică parola doar pentru Controlul parental**. Pe de altă parte, dacă parola a fost configurată doar pentru Controlul parental și debifați această opțiune, parola respectivă va fi cerută la configurarea oricărei opțiuni BitDefender.

Important
Dacă uitați parola va fi nevoie să reparați produsul pentru a schimba configurarea BitDefender.

- **Întreabă dacă doresc să setez parola atunci când activez Controlul parental** - vă solicită să configurați parola atunci când doriți să activați Controlul parental, dacă aceasta nu este configurată. Setând parola, veți împiedica alți utilizatori cu drepturi administrative pe sistem să modifice setările de Control parental pe care le-ați configurat pentru un anumit utilizator.
- **Afișează știri BitDefender (avertizări de securitate)** - afișează din când în când notificări de securitate referitoare la noi viruși descoperiți, trimise de serverul BitDefender.
- **Afișează ferestre pop-up (note pe ecran)** - afișează ferestre de informare cu privire la starea produsului. Puteți configura BitDefender să afișeze ferestre pop-up numai atunci când interfața este în Modul Novice/Intermediar sau Expert.
- **Afișează bara de scanare (graficul de pe ecran al activității produsului)** - afișează Bara de scanare atunci când vă conectați la Windows. Debifați această căsuță dacă nu doriți ca bara de scanare să mai fie afișată.



Bara de scanare

Notă
Această opțiune poate fi configurată doar pentru contul de utilizator Windows curent. Bara de scanare este disponibilă numai atunci când interfața este în Modul Expert.

17.2.2. Setări raportare viruși

- **Trimite rapoarte virusi** - trimite Laboratorului BitDefender rapoarte referitoare la virușii identificați în calculatorul dumneavoastră. Astfel ne ajutați să ținem evidența noilor viruși.

  Rapoartele nu conțin date confidențiale, precum numele dumneavoastră, adresa IP sau altele, și nu vor fi folosite în scopuri comerciale. Informațiile trimise vor conține doar numele virușilor și vor fi folosite doar pentru a crea rapoarte statistice.

- **Activează Detecția epidemiilor virale de către BitDefender** - trimite Laboratorului BitDefender rapoarte referitoare la potențiale epidemii virale.

  Rapoartele nu conțin date confidențiale, precum numele dumneavoastră, adresa IP sau altele, și nu vor fi folosite în scopuri comerciale. Informațiile trimise vor conține doar potențialul virus și vor fi folosite doar pentru a detecta noi viruși.

17.3. Informații sistem

BitDefender vă permite să vedeți, dintr-un singur loc, toate setările de sistem și aplicațiile înregistrate să ruleze la pornirea sistemului. Astfel, puteți monitoriza activitatea sistemului și a aplicațiilor instalate pe acesta și identifica posibile infecții ale sistemului.

Pentru a obține informații legate de sistem, mergeți la **General>Info sistem** în Modul Expert.

Informații sistem

Lista conține toate obiectele încărcate la pornirea sistemului precum și obiectele încărcate de diverse aplicații.

Sunt disponibile trei butoane:

- **Restaurează** - modifică o asociere de fișiere curentă cu asocierea de fișiere implicită. Disponibil doar pentru setările **Asocieri de fișiere**!
- **Mergi la** - deschide o fereastră unde obiectul selectat este plasat (de exemplu, **Regiștrii**).

  Notă
  În funcție de elementul selectat, este posibil ca butonul **Mergi la** să nu apară.

- **Actualizează** - redeschide secțiunea **Info sistem**.

18. Antivirus

BitDefender vă protejează calculatorul împotriva oricăror amenințări malițioase (viruși, troieni, aplicații spyware, rootkituri și altele). Protecția oferită de BitDefender se împarte în două categorii:

- Protecția în timp real - previne pătrunderea noilor amenințări malware în sistemul dumneavoastră. BitDefender va scana, de exemplu, un document Word atunci când îl deschideți și un mesaj e-mail atunci când îl primiți.

  Notă
  Protecția în timp real mai este denumită și scanare la acces - fișierele sunt scanate în timp ce utilizatorii le accesează.

- Scanarea la cerere - permite detectarea și ștergerea aplicațiilor malițioase care există deja în sistemul dumneavoastră. Acesta este modul clasic de scanare, inițiată de utilizator – dumneavoastră alegeți partițiile, directoarele sau fișierele pe care trebuie să le scaneze BitDefender, iar BitDefender le scanează – la cerere. Sarcinile de scanare permit crearea unor rutine de scanare personalizate și pot fi programate să ruleze periodic.

18.1. Protecție în timp real

BitDefender oferă protecție continuă în timp real împotriva unui număr mare de amenințări malițioase scanând toate fișierele accesate, mesajele e-mail și comunicațiile prin programe de mesagerie instantă (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). BitDefender Antiphishing împiedică dezvăluirea informațiilor personale în timp ce navigați pe Internet alertându-vă despre paginile web cu conținut potențial phishing.

Pentru a configura protecția în timp real și BitDefender Antiphishing, mergeți la **Antivirus>Scut** în Modul Expert.

Protecție în timp real

Puteți vedea dacă protecția în timp real este activată sau nu. Pentru a schimba starea protecției în timp real, debifați sau selectați căsuța corespunzătoare.

Important

Pentru a preveni infectarea calculatorului personal cu viruși, păstrați **Protectia in timp real** activată.

Pentru a iniția o scanare de sistem, faceți clic pe **Scanează acum**.

18.1.1. Configurarea nivelului de protecție

Puteți alege nivelul de protecție adecvat nevoilor dumneavoastră de securitate. Mutați cursorul pentru a seta nivelul de protecție dorit.

Există trei nivele de protecție:

Nivel de protecție	Descriere
Permisiv	Acoperă nevoile elementare de securitate. Consumul de resurse este foarte scăzut.

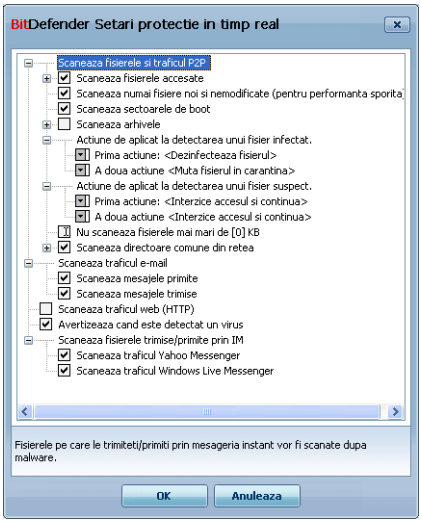
Nivel de protecție	Descriere
	Numai aplicațiile și mesajele e-mail primite sunt scanate împotriva virușilor. Pe lângă metoda clasică de scanare bazată pe semnături, se utilizează și analiza euristică. Acțiunile aplicate fișierelor infectate sunt următoarele: dezinfectare/mutare în carantină.
Standard	Oferă protecție standard. Consumul de resurse este scăzut. Toate fișierele și mesajele e-mail, primite&trimise sunt scanate împotriva virușilor și a aplicațiilor. Pe lângă metoda clasică de scanare bazată pe semnături, se utilizează și analiza euristică. Acțiunile aplicate fișierelor infectate sunt următoarele: dezinfectare/trimitere în carantină.
Agresiv	Oferă protecție avansată. Consumul de resurse este moderat. Toate fișierele și mesajele e-mail,l, primite&trimise, precum și traficul web, sunt scanate împotriva virușilor și a aplicațiilor. Pe lângă metoda clasică de scanare bazată pe semnături, se utilizează și analiza euristică. Acțiunile aplicate fișierelor infectate sunt următoarele: dezinfectare/trimitere în carantină.

Pentru a aplica setările implicite ale protecției în timp real, faceți clic pe **Nivel implicit**.

18.1.2. Personalizarea nivelului de protecție

Utilizatorii avansați pot folosi și modifica opțiunile de scanare oferite de BitDefender în beneficiul lor. Motorul de scanare poate fi setat să scaneze doar anumite extensii de fișiere, să caute anumite tipuri de amenințări malițioase sau să nu scaneze arhivele. Aceasta poate reduce cu mult timpul de scanare, precum și viteza de reacție a sistemului pe durata scanării.

Puteți personaliza **Protecția în timp real** facând clic pe **Nivel personal**. Va apărea următoarea fereastră:



Setări Scut

Opțiunile de scanare sunt organizate intr-un meniu expandabil similar celor din Windows. Faceți clic pe semnul “+” pentru a deschide o opțiune sau pe semnul “-” pentru a închide o opțiune.

Notă

Puteți observa că, deși semnul “+” apare, unele opțiuni de scanare nu pot fi deschise. Motivul este că aceste opțiuni nu au fost selectate încă.Dacă veți selecta aceste opțiuni, acestea vor putea fi deschise.

- **Opțiuni de scanare a fișierelor și a transferurilor P2P** - scanează fișierele accesate și comunicația prin programe de mesagerie instantă (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). În continuare, selectați tipurile de fișiere care doriți să fie scanate.

Opțiune		Descriere
Scanează fișiere accesate	**Scanează toate fisierele**	Vor fi scanate toate fișierele accesate, indiferent de tipul lor.
	Scanează doar aplicații	Nu vor fi scanate decât fișierele program, și anume fișierele cu următoarele extensii: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc;

Opțiune		Descriere
		.dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml și .nws.
	Scanează extensiile definite de utilizator	Nu vor fi scanate decât fișierele cu extensiile specificate de utilizator. Aceste extensii trebuie separate prin ";".
	Scanează după soft cu risc	Scanează după aplicații care prezintă un potențial risc (riskware). Fișierele detectate vor considerate ca fiind infectate. Programele care includ componente adware se pot opri din funcționare dacă această opțiune este activată. Selectați **Omitere dialere și aplicații de la scanare** și/sau **Omitere keyloggere de la scanare** dacă doriți să excludeți aceste tipuri de fișiere de la scanare.
Scanează doar fișiere noi sau modificate		Scanează numai fișierele care nu au fost scanate niciodată sau care sunt modificate față de ultima dată când au fost scanate. Selectând această opțiune, puteți îmbunătăți performanța sistemului cu un risc minim pentru securitatea acestuia.
Scanează sectorul de boot		Scanează sectorul de boot al sistemului.
Deschide arhive		Vor fi scanate și arhivele accesate. Selectând această opțiune, performanțele calculatorului vor scădea. Puteți stabili dimensiunea maximă a arhivelor de scanat (în kilobiți, introduceți 0 dacă doriți să fie scanate toate arhivele) și adâncimea maximă până la care va avea loc scanarea.
Prima acțiune		Selectați din meniu prima acțiune ce va fi luată asupra fișierelor infectate sau suspecte.
	Interzice accesul si continua	În caz că un fișier este infectat, accesul la acesta va fi interzis.

Opțiune		Descriere
	Dezinfectează fișier	Elimină codul malițios din fișierele infectate.
	Dezinfecteaza fisier	Șterge imediat fișierele infectate, fără niciun avertisment.
	Mută fișierele infectate în carantină	Mută fișierele infectate în carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.
A doua acțiune		Selectați din meniu a doua acțiune pentru fișierele infectate sau suspecte, în caz că prima acțiune eșuează.
	Interzice accesul si continua	În caz că un fișier este infectat, accesul la acesta va fi interzis.
	Dezinfecteaza fisier	Șterge imediat fișierele infectate, fără niciun avertisment.
	Mută fișierele infectate în carantină	Mută fișierele infectate în carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.
Nu scana fișiere mai mari de [x] Kb		Introduceți dimensiunea maximă a fișierelor ce vor fi scanate. Dacă dimensiunea este de 0 Kb, toate fișierele vor fi scanate, indiferent de mărimea lor.
Scanează fișiere partajate în rețea	**Scanează toate fisierele**	Vor fi scanate toate fișierele accesate din rețea, indiferent de tipul lor.
	Scanează doar aplicații	Nu vor fi scanate decât fișierele program, și anume fișierele cu următoarele extensii: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml` și `.nws`.

Opțiune		Descriere
	Scanează extensiile definite de utilizator	Nu vor fi scanate decât fișierele cu extensiile specificate de utilizator. Aceste extensii trebuie separate prin ";".

- **Scanează traficul e-mail** - scanează traficul e-mail.

  Următoarele opțiuni sunt disponibile:

Opțiune	Descriere
Scanează mesajele e-mail primite	Scanează toate mesajele primite.
Scanează mesajele e-mail trimise	Scanează toate mesajele trimise.

- **Scanează traficul web (HTTP)** - scanează tot traficul web.
- **Avertizeaza cand este detectat un virus** - afișează o fereastră de avertizare la descoperirea unui virus într-un fișier sau mesaj e-mail.

  Pentru fișierele infectate fereastra de avertizare va conține calea și numele virusului, acțiunea luată de BitDefender și un link către site-ul BitDefender, unde puteți afla mai multe informații despre virus. Pentru mesajele infectate fereastra de avertizare va conține contain și informații despre expeditor și destinatar.

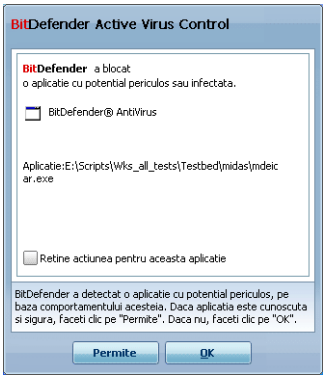
  Dacă este detectat un fișier suspect, din fereastra de alertă puteți lansa un program asistent ce vă va ajuta să trimiteți acest fișier Laboratorului BitDefender pentru analiză aprofundată. Pentru a primi informații despre acest fișier introduceți adresa dumneavoastră de e-mail.
- **Scanează fișierele primite/trimise prin IM.** Pentru a scana fișierele trimise sau primite prin intermediul Yahoo Messenger sau Windows Live Messenger, selectați căsuțele corespunzătoare.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

18.1.3. Configurarea setărilor Active Virus Control

Tehnologia BitDefender Active Virus Control oferă un nou nivel de protecție împotriva amenințărilor noi, pentru care încă nu au fost lansate semnături. Acesta monitorizează și analizează în mod constant comportamentul aplicațiilor care rulează pe calculatorul dumneavoastră și vă alertează dacă o aplicație are un comportament suspicios.

Tehnologia Active Virus Control poate fi configurată să vă alerteze și să vă ceară să acționați ori de câte ori o aplicație încearcă să efectueze o acțiune cu potențial periculos.



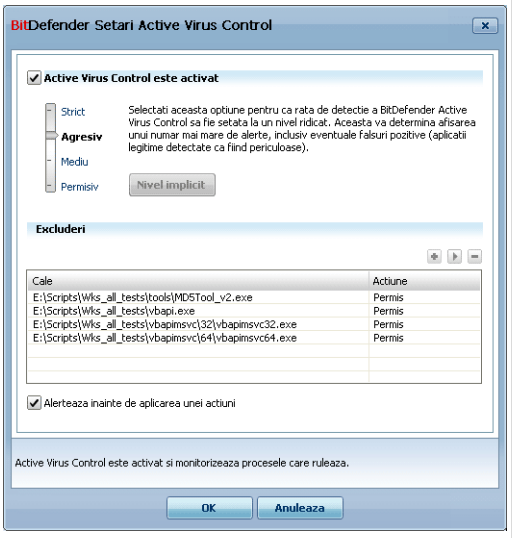
Alerta Active Virus Control

Dacă aplicația detectată este cunoscută, faceți clic pe **Permite**.

Dacă doriți să închideți imediat aplicația, faceți clic pe **OK**.

Selectați căsuța **Reține acțiunea pentru această aplicație** înainte de a face selecția și BitDefender va aplica aceeași acțiune la detectarea ulterioară a aplicației. Regula creată astfel va fi afișată în fereastra de configurare a Active Virus Control.

Pentru a configura Active Virus Control, faceți clic pe **Setări avansate**.



Setări Active Virus Control

Selectați căsuța corespunzătoare pentru a activa Active Virus Control.

Important

Mențineți Active Virus Control activat pentru protecție împotriva virușilor necunoscuți.

Dacă doriți să fiți alertat și vi se solicite să acționați de către Active Virus Control ori de câte ori o aplicație încearcă să efectueze o acțiune cu potențial periculos, selectați căsuța **Întreabă-mă înainte de a aplica o acțiune**.

Configurarea nivelului de protecție

Nivelul de protecție asigurat de Active Virus Control se schimbă automat atunci când stabiliți un nou nivel al protecției în timp real. Dacă nu vă mulțumește setarea implicită, puteți configura manual nivelul de protecție.

Notă

Rețineți că modificarea nivelului de protecție în timp real va determina modificarea nivelului de protecție oferit de Active Virus Control. Dacă setați protecția în timp real la nivelul **Permisiv**, Active Virus Control va fi dezactivat în mod automat. În acest caz, dacă doriți să folosiți Active Virus Control, puteți să-l activați manual.

Mutați cursorul pentru a seta nivelul de protecție adecvat nevoilor dumneavoastră de securitate.

Nivel de protecție	Descriere
Critic	Monitorizarea strictă a tuturor aplicațiilor pentru identificarea acțiunilor cu potențial periculos.
Standard	Ratele de detecție sunt mari și sunt posibile rezultate fals pozitive.
Mediu	Monitorizarea aplicațiilor se face la nivel mediu și pot apărea câteva rezultate fals pozitive.
Permisiv	Ratele de detecție sunt mici și nu există rezultate fals pozitive.

Administrarea aplicațiilor sigure/nesigure

Puteți adăuga aplicații cunoscute și în care aveți încredere pe lista de aplicații sigure. Aceste aplicații nu vor mai fi verificate de BitDefender Active Virus Control și li se va permite accesul în mod automat.

Aplicațiile pentru care ați creat reguli apar în tabelul **Excepții**. Pentru fiecare regulă, sunt afișate calea către aplicație și acțiunea pe care ați stabilit-o pentru aceasta (Permite sau Blochează).

Pentru a schimba acțiunea corespunzătoare unei aplicații, faceți clic pe acțiunea curentă și selectați acțiunea dorită din meniu.

Pentru administrarea listei, folosiți butoanele de deasupra tabelului:

- **Adăugă** - adăugă o nouă aplicație pe listă.
- **Elimină** - elimină o aplicație din lista.
- **Editează** - editează o regula pentru aplicații.

18.1.4. Dezactivarea protecției în timp real

Dacă doriți să dezactivați protecția în timp real, va apărea o fereastră de avertizare. Va trebui să confirmați acțiunea selectând din meniu intervalul de timp pentru care să fie dezactivată protecția în timp real. Puteți dezactiva protecția în timp real pentru 5, 15 sau 30 minute, pentru o oră, permanent sau doar până la repornirea sistemului.

Avertisment

Aceasta este o problemă majoră de securitate. Vă recomandăm să dezactivați protecția în timp real pentru cât mai puțin timp posibil. Dacă protecția în timp real este dezactivată, nu veți mai fi protejat împotriva amenințărilor malițioase.

18.1.5. Configurarea protecției antiphishing

BitDefender furnizează protecție antiphishing în timp real pentru:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

Puteți alege să dezactivați protecția antiphishing complet sau doar pentru anumite aplicații.

Puteți face clic pe **Lista albă** pentru a configura și administra lista paginilor web care nu sunt verificate de motoarele antiphishing ale BitDefender.

Lista albă antiphishing

Puteți vedea site-urile web care nu sunt verificate de motoarele antiphishing ale BitDefender.

Pentru a adăuga un nou site web pe lista albă, introduceți adresa acestuia în câmpul **Adresă nouă** și faceți clic pe **Adaugă**. Este recomandat ca lista albă să conțină numai site-uri web în care aveți deplină încredere. De exemplu, adăugați site-urile web de unde cumpărați produse online.

Notă

Puteți adăuga ușor site-uri web pe lista albă din bara de comenzi BitDefender Antiphishing integrată în browserul dumneavoastră. Pentru mai multe informații, consultați *„Integrarea cu browserele web”* (p. 288).

Pentru a șterge un site din lista albă, faceți clic pe butonul **Șterge** corespunzător.

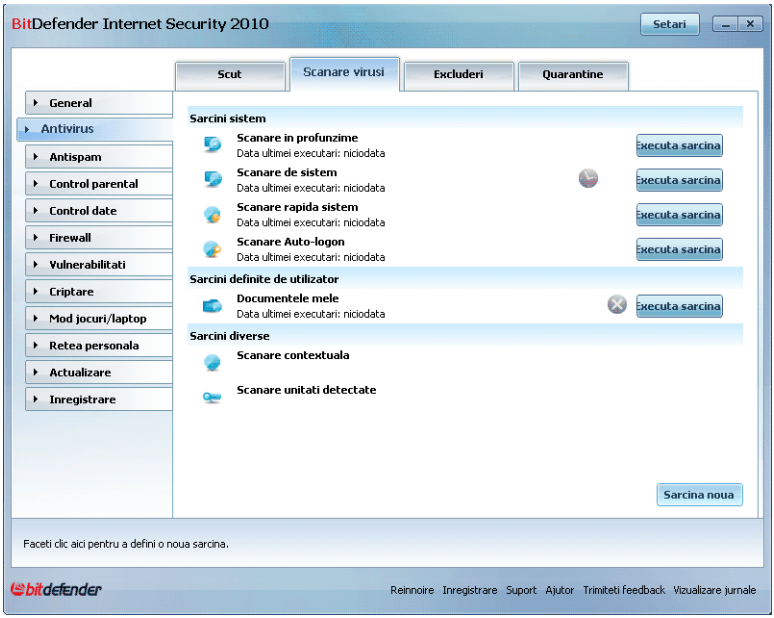
Faceți clic pe **Save** pentru a salva modificările și închide fereastra.

18.2. Scanarea la cerere

Principalul obiectiv BitDefender este protejarea calculatorului dumneavoastră de viruși. Aceasta se face în primul rând nepermițând virușilor noi să pătrundă în sistem, prin scanarea mesajele e-mail și a fișierelor descărcate sau copiate pe calculator.

Există însă riscul ca un virus să fi fost în sistem înainte de instalarea BitDefender. Din acest motiv, este indicat să vă scanați calculatorul de viruși după instalarea BitDefender. Și este, de asemenea, recomandat să vă scanați sistemul periodic.

Pentru a configura și iniția scanarea la cerere, mergeți la **Antivirus>Scanare viruși** în Modul Expert.



Sarcini de scanare

Scanarea la cerere se bazează pe sarcini de scanare. Sarcinile de scanare sunt cele care specifică opțiunile de scanare și obiectele care să fie scanate. Puteți scana calculatorul oricând doriți rulând sarcinile de scanare predefinite sau propriile dumneavoastră sarcini de scanare (sarcini definite de utilizator). De asemenea, puteți programa sarcinile să ruleze periodic sau când sistemul nu este utilizat, pentru a nu interfera cu munca dumneavoastră.

18.2.1. Sarcini de scanare

BitDefender este dotat cu o serie de sarcini predefinite, ce acoperă nevoile comune de securitate. Pe lângă acestea, puteți crea propriile dumneavoastră sarcini de scanare personalizate.

Există trei categorii de sarcini de scanare:

- **Sarcini sistem** - conține lista sarcinilor implicite de sistem. Următoarele sarcini sunt disponibile:

Sarcină implicită	Descriere
Scanare profundă sistem	Scanează întregul sistem. În configurația implicită, se scanează după toate tipurile de aplicații malițioase care amenință securitatea sistemului dumneavoastră, cum ar fi virușii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) și altele.
Scanare de sistem	Scanează întregul sistem, cu excepția arhivelor. În configurația implicită, scanează după toate tipurile de aplicații periculoase, altele decât cele de tip rootkit.
Scanare rapidă sistem	Scanează directoarele `Windows` și `Program Files`. În configurația implicită, se scanează după toate tipurile de aplicații malițioase, mai puțin cele ascunse (rootkituri), dar nu sunt scanate memoria, regiștrii și fișierele cookie.
Scanare automată la conectare	Scanează obiectele executate atunci când un utilizator se conectează la Windows. În mod implicit, scanarea autologon este dezactivată. Dacă doriți să folosiți această sarcină, faceți clic-dreapta pe ea, selectați **Planificare** și stabiliți ca sarcina să fie rulată **la pornire sistem**. Puteți indica după cât timp de la pornirea sistemului să fie rulată sarcina (în minute).

Notă

Deoarece sarcinile **Scanare profundă sistem** și **Scanare completă sistem** analizează întregul sistem, procesul poate fi unul de durată. De aceea, vă recomandăm să rulați aceste sarcini cu prioritate scăzută sau chiar atunci când nu utilizați calculatorul.

- **Sarcini utilizator** - conține sarcinile definite de utilizator.

  O sarcină denumită `Documentele mele` este furnizată. Utilizați această sarcină pentru a scana directoare importante ale utilizatorului curent: `My Documents`, `Desktop` și `StartUp`. Astfel, veți asigura siguranța documentelor dumneavoastră, un spațiu de lucru sigur și rularea la pornirea sistemului a unor aplicații necompromise.

- **Sarcini diverse** - conține o listă de sarcini de scanare diverse. Aceste sarcini de scanare se referă la tipuri alternative de scanare ce nu pot fi rulate din această fereastră. Puteți doar să modificați setările acestora și să examinați rapoartele de scanare.

Fiecare sarcină are o fereastră de **Proprietăți** în care o puteți configura și puteți vedea jurnalele de scanare. Pentru a deschide această fereastră, faceți dublu-clic pe sarcină sau faceți clic pe butonul **Proprietăți** din fața numelui fiecărei sarcini. Pentru mai multe informații, consultați secțiunea *„Configurarea sarcinilor de scanare"* (p. 143).

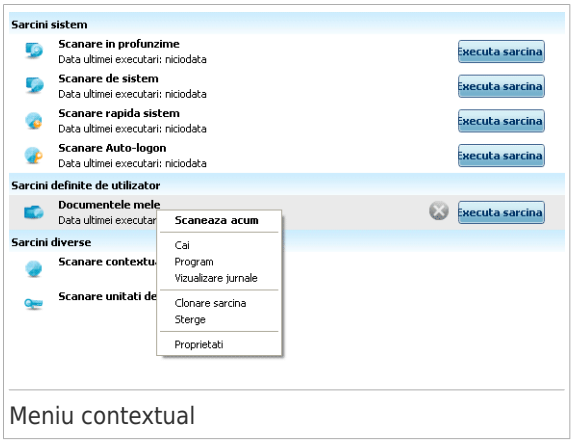
Pentru a rula o sarcină de scanare a sistemului sau definită de utilizator, faceți clic pe butonul **Rulează sarcina** corespunzător. Va apărea programul asistent de scanare care vă va ghida de-a lungul procesului de scanare.

Atunci când o sarcină este planificată să ruleze automat, la un moment ulterior sau în mod regulat, butonul **Planifica** este afișat în partea dreaptă a acesteia. Faceți clic pe acest buton pentru a deschide fereastra **Proprietăți**, tabul Planificare, în care puteți vedea și modifica planul de rulare a sarcinii.

Dacă nu mai aveți nevoie de una dintre sarcinile de scanare pe care le-ați creat (o sarcină definită de utilizator), o puteți șterge făcând clic pe butonul **Șterge** din dreapta acesteia. Nu puteți elimina sarcinile de sistem sau sarcinile diverse.

18.2.2. Utilizarea meniului contextual

Un meniu contextual este disponibil pentru fiecare sarcină. Faceți clic-dreapta pe o sarcină selectată pentru a-l deschide.



Meniu contextual

Pentru sarcinile de sistem și definite de utilizator, sunt disponibile următoarele comenzi în meniul de scurtături:

- **Scanare** - rulează sarcina selectată, lansând o scanare imediată.
- **Căi** - deschide fereastra de **Proprietăți** la tabul Căiîn care puteți modifica ținta sarcinii de scanare selectate.

Notă
În cazul sarcinilor de sistem, această opțiune este înlocuită cu **Arată locații scanare** deoarece puteți vedea numai locațiile scanate.

- **Planificare** - deschide fereastra de **Proprietăți** la tabul Planificare, în care puteți programa sarcina selectată.
- **Vizualizare jurnale** - deschide fereastra de **Proprietăți** la tabul Jurnale, unde puteți examina rapoartele generate la fiecare rulare a sarcinii selectate.
- **Clonează sarcina** - creează o copie a sarcinii selectate. Acest lucru este util în crearea de noi sarcini, deoarece puteți modifica setările duplicatului unei sarcini.
- **Șterge** - șterge sarcina selectată.

Notă
Nu este disponibil pentru sarcinile de sistem. Nu puteți șterge o sarcină de sistem.

- **Proprietăți** - deschide fereastra de **Proprietăți** la tabul Setări, unde puteți modifica setările sarcinii selectate.

Datorită caracterului special al sarcinilor din categoria **Sarcini diverse**, numai opțiunile **Vizualizare jurnale** și **Proprietăți** sunt disponibile în acest caz.

18.2.3. Crearea sarcinilor de scanare

Pentru a crea o sarcină de scanare, utilizați una dintre următoarele metode:

- Clonați o sarcină existentă, redenumiți-o și faceți modificările necesare în fereastra de Proprietăți.
- Faceți clic pe **Sarcină nouă** pentru a crea o nouă sarcină și a o configura.

18.2.4. Configurarea sarcinilor de scanare

Fiecare sarcină de scanare are propria fereastră de **Proprietăți**, unde puteți configura opțiunile de scanare, puteți alege obiectele ce vor fi scanate, puteți planifica sarcina sau examina rapoartele. Pentru a accesa această fereastră, faceți clic pe butonul **Proprietăți** din stânga sarcinii (sau faceți clic dreapta pe sarcină și apoi clic pe **Proprietăți**). De asemenea, puteți face dublu-clic pe sarcină.

Notă
Pentru mai multe informații despre vizualizarea rapoartelor și tabul **Rapoarte**, consultați *„Examinarea rapoartelor de scanare”* (p. 163).

Configurarea setărilor de scanare

Pentru a configura opțiunile de scanare ale unei anumite sarcini de scanare, faceți clic-dreapta pe aceasta și selectați **Proprietăți**. Va apărea următoarea fereastră:

Descriere generală

Aici puteți vedea informații cu privire la sarcină (nume, când a rulat ultima dată și programul de rulare) și puteți configura setările de scanare.

Alegerea nivelului de scanare

Puteți configura ușor setările de scanare alegând nivelul de scanare. Mutați cursorul pentru a seta nivelul de scanare dorit.

Există trei nivele de scanare:

Nivel de protecție	Descriere
Permisiv	Oferă o rată de detecție moderată. Consumul de resurse este scăzut. Numai programele sunt scanate împotriva virușilor. Pe lângă metoda clasică de scanare bazată pe semnături, se utilizează și analiza euristică.
Mediu	Oferă o rată de detecție bună. Consumul de resurse este moderat.

Nivel de protecție	Descriere
	Toate aplicațiile sunt scanate împotriva virușilor și a aplicațiilor spyware. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează și analiza euristică.
Agresiv	Oferă o rată de detecție ridicată. Consumul de resurse este și el ridicat. Toate aplicațiile și arhivele sunt scanate împotriva virușilor și a aplicațiilor spyware. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează și analiza euristică.

Sunt de asemenea disponibile și o serie de opțiuni generale privind procesul de scanare:

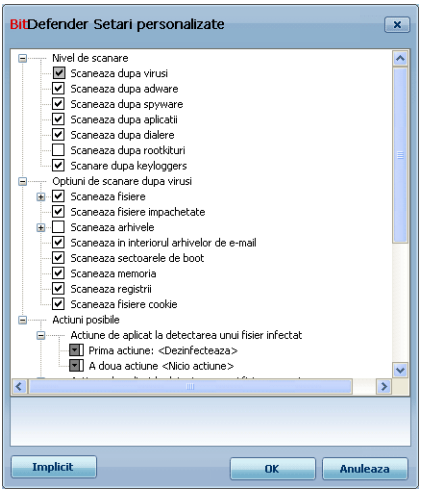
- **Executa procesul cu prioritate scăzută.** Reduce prioritatea procesului de scanare. Veți permite altor programe să ruleze cu o viteză superioară, dar timpul necesar pentru finalizarea scanării va crește.
- **Minimizează asistentul de scanare la bara de sistem.** Minimizează fereastra de scanare bara de sistem. Faceți dublu-clic pe simbolul BitDefender pentru a o deschide.
- **Închide calculatorul la finalizarea scanării dacă nu este detectată nicio amenințare**

Faceți clic pe **OK** pentru a salva modificările și închide fereastra. Pentru a executa sarcina faceți clic pe **Scanează**.

Personalizarea nivelului de scanare

Utilizatorii avansați pot folosi și modifica opțiunile de scanare oferite de BitDefender în beneficiul lor. Motorul de scanare poate fi setat să scaneze doar anumite extensii de fișiere, să caute anumite tipuri de amenințări malițioase sau să nu scaneze arhivele. Aceasta poate reduce cu mult timpul de scanare, precum și viteza de reacție a sistemului pe durata scanării.

Faceți clic pe **Personalizat** pentru a vă seta propriile opțiuni de scanare. Va apărea o nouă fereastră.



Setări de Scanare

Opțiunile de scanare sunt organizate intr-un meniu expandabil similar celor din Windows. Faceți clic pe semnul “+” pentru a deschide o opțiune sau pe semnul “-” pentru a închide o opțiune.

Opțiunile de scanare sunt grupate în trei categorii:

- **Nivel scanare.** Specificați tipul de aplicații malițioase după care să scaneze BitDefender, selectând opțiunile adecvate din categoria **Nivel scanare**.

Opțiune	Descriere
Scanează după viruși	Scanează după viruși cunoscuți. BitDefender detectează, de asemenea, și corpurile incomplete de viruși, îndepărtând astfel orice posibilă amenințare ce ar putea afecta securitatea sistemului dumneavostră.
Scanează după adware	Scanează după amenințări adware. Fișierele detectate vor fi considerate ca fiind infectate. Programele care includ componente adware se pot opri din funcționare dacă această opțiune este activată.
Scanează după spyware	Scanează după amenințări spyware cunoscute. Fișierele detectate vor fi considerate ca fiind infectate.

Opțiune	Descriere
Scanează după aplicații	Scanează după aplicații legitime care pot fi folosite pentru a spiona, pentru a ascunde aplicații malițioase sau cu alte intenții răuvoitoare.
Scanează după dialere	Scanează după aplicații care apelează numere cu cost ridicat. Fișierele detectate vor fi considerate ca fiind infectate. Programele care includ componente adware se pot opri din funcționare dacă această opțiune este activată.
Scanare după rootkituri	Scanează după obiecte ascunse (fișiere și procese), cunoscute sub denumirea generică de rootkituri.

- **Opțiuni scanare după viruși.** Specificați tipurile de obiecte care vor fi scanate (tipuri de fișiere, arhive și altele) selectând opțiunile adecvate din categoria **Opțiuni scanare după viruși**.

Opțiune		Descriere
Scanează fișiere	**Scanează toate fișierele**	Toate fișierele sunt scanate, indiferent de tipul lor.
	Scanează numai programele	Nu vor fiscanate decât fișierele program, și anume fișierele cu următoarele extensii: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`; `prc`; `url`; `smm`; `pdf`; `msi`; `ini`; `csc`; `cmd`; `bas`; `eml` și `nws`.
	Scanează extensiile definite de utilizator	Nu vor fi scanate decât fișierele cu extensiile specificate de utilizator. Aceste extensii trebuie separate prin ";".
Deschide programe impachetate		Scanează programele împachetate.
Deschide arhive		Scanează în interiorul arhivelor normale, precum `.zip`, `.rar`, `.ace`, `.iso` și altele. Selectați căsuța **Scanează aplicațiile de instalare și arhivele chm** dacă doriți să fie scanate aceste tipuri de fișiere.

Opțiune	Descriere
	Scanarea fișierelor arhivate necesită mai mult timp și mai multe resurse de sistem. Puteți stabili dimensiunea maximă a arhivelor de scanat, în kilobiți (KB), introducând valoarea corespunzătoare in câmpul **Limitează dimensiunea arhivelor scanate la**.
Scanează în arhivele de e-mail	Scanează în interiorul arhivelor de e-mail.
Scanează sectorul de boot	Scanează sectorul de boot al sistemului.
Scanare memorie	Scanează memoria împotriva virușilor și a altor aplicații malițioase.
Scanează regiștri	Scanează intrările din regiștri.
Scanează fișiere cookie	Scanează fișierele cookie.

- **Optiuni de acțiune .** Specificați acțiunile care vor fi aplicate fiecărei categorii de fișiere detectate, folosind opțiunile din această categorie.

  Notă

  Pentru a stabili o nouă acțiune, faceți clic pe **Prima acțiune** curentă și selectați opțiunea dorită din meniu. Specificați o **A doua acțiune** care va fi aplicată dacă prima eșuează.

  ▶ Selectați acțiunea ce trebuie aplicată fișierelor infectate detectate. Următoarele opțiuni sunt disponibile:

Acțiune	Descriere
Nicio acțiune	Nici se va efectua nici o acțiune în legătură cu fișierelor infectate. Aceste fișiere vor apărea în fișierul de raport.
Dezinfectează	Elimină codul malware din fișierele infectate detectate.
Șterge	Șterge imediat fișierele infectate, fără niciun avertisment.
Mută în carantină	Mută fișierele infectate în carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.

  ▶ Selectați acțiunea ce trebuie aplicată fișierelor detectate ca fiind infectate. Următoarele opțiuni sunt disponibile:

Acțiune	Descriere
Nicio acțiune	Nicio acțiune nu va fi aplicată fișierelor suspecte. Aceste fișiere vor apărea în fișierul de raport.
Șterge	Șterge imediat fișierele suspecte, fără niciun avertisment.
Mută în carantină	Mută fișierele suspecte în carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.

Notă

Fișierele pot fi detectate ca fiind suspecte în urma analizei euristice. Vă recomandăm să trimiteți aceste fișiere Laboratorului BitDefender.

- Selectați acțiunea ce va fi aplicată fișierelor ascunse (rootkituri) detectate. Următoarele opțiuni sunt disponibile:

Acțiune	Descriere
Nicio acțiune	Nicio acțiune nu va fi aplicată fișierelor ascunse. Aceste fișiere vor apărea în fișierul de raport.
Redenumește	Redenumește fișierele ascunse adăugând extensia `.bd.ren` la numele acestora. Ca urmare, veți putea căuta și găsi astfel de fișiere pe calculatorul dumneavoastră, dacă există.
Mută în carantină	Mută fișierele ascunse în carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.

Notă

Aceste fișiere ascunse nu sunt fișierele pe care le ascundeți deliberat din Windows. Ele sunt fișiere ascunse cu ajutorul unor programe speciale, cunoscute sub numele de rootkituri. Rootkiturile nu sunt în sine programe malițioase. Totuși, ele sunt utilizate frecvent pentru a împiedica detectarea virușilor sau aplicațiilor spion de către programele antivirus obișnuite.

- **Opțiuni de acțiune pentru fișiere protejate prin parolă sau criptate.** Fișierele criptate prin intermediul Windows pot fi importante pentru dumneavoastră. Acesta este motivul pentru care puteți configura acțiuni diferite pentru a fi aplicate fișierelor infectate sau suspecte care sunt criptate prin intermediul Windows. O altă categorie de fișiere care necesită acțiuni speciale sunt arhivele protejate prin parolă. Arhivele protejate prin parolă nu pot fi scanate decât dacă furnizați parola. Utilizați aceste opțiuni pentru a configura

acțiunile care trebuie aplicate arhivelor protejate prin parolă și fișierelor criptate prin intermediul Windows.

- **Acțiune aplicată la detectarea unui fișier criptat infectat.** Selectați acțiunea care va fi aplicată fișierelor infectate care sunt criptate prin intermediul Windows. Următoarele opțiuni sunt disponibile:

Acțiune	Descriere
Nicio acțiune	Fișierele infectate care sunt criptate prin intermediul Windows vor fi numai înregistrate în raportul de scanare. După finalizarea scanării, puteți deschide raportul de scanare pentru a vedea informații despre aceste fișiere.
Dezinfectează	Elimină codul malware din fișierele infectate detectate. Dezinfectarea poate eșua în anumite cazuri, ca de exemplu atunci când fișierul infectat se află într-o anumită arhivă de mail.
Șterge	Șterge imediat fișierele infectate de pe disc, fără niciun avertisment.
Mută în carantină	Mută fișierele infectate din locația originală în directorul carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.

- **Acțiune aplicată la detectarea unui fișier criptat suspect.** Selectați acțiunea care va fi aplicată fișierelor suspecte care sunt criptate prin intermediul Windows. Următoarele opțiuni sunt disponibile:

Acțiune	Descriere
Nicio acțiune	Fișierele suspecte care sunt criptate prin intermediul Windows vor fi numai înregistrate în raportul de scanare. După finalizarea scanării, puteți deschide raportul de scanare pentru a vedea informații despre aceste fișiere.
Șterge	Șterge imediat fișierele suspecte, fără niciun avertisment.
Mută în carantină	Mută fișierele suspecte în carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.

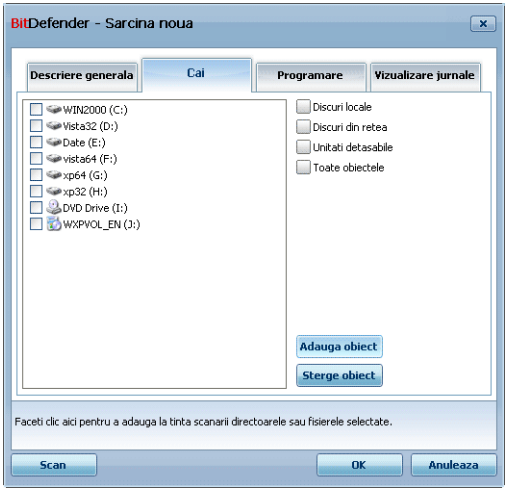
– **Acțiune aplicată la detectarea unui fișier protejat prin parolă.** Selectați acțiunea care trebuie aplicată fișierelor protejate prin parolă detectate. Următoarele opțiuni sunt disponibile:

Acțiune	Descriere
Log only	Doar ține evidența fișierelor protejate prin parolă în raportul de scanare. După finalizarea scanării, puteți deschide raportul de scanare pentru a vedea informații despre aceste fișiere.
Cere parola	Atunci când este detectat un fișier protejat prin parolă, cere utilizatorului să furnizeze parola pentru a putea scana fișierul.

Dacă faceți clic pe **Implicit** veți încărca setările standard. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Setarea locației de scanare

Pentru a stabili ținta unei anumite sarcini de scanare, faceți clic-dreapta pe sarcină și selectați **Căi**. Dacă sunteți deja în fereastra Proprietăți a sarcinii, selectați tabul **Căi**. Va apărea următoarea fereastră:



Locație scanare

Puteți vedea lista partițiilor locale, de rețea și amovibile (unitatea floppy, CD/DVD), precum și fișierele și directoarele adăugate anterior, dacă există. Toate obiectele bifate vor fi scanate atunci când este rulată sarcina.

Următoarele butoane sunt disponibile:

- **Adaugă obiect(e)** - deschide o fereastră de explorare din care puteți selecta fișierele sau directoarele care doriți să fie scanate.

Notă
Puteți folosi drag & drop pentru a adăuga fișiere/directoare la listă.

- **Șterge obiect(e)** - șterge fișierele / directoarele care au fost selectate anterior din lista de obiecte de scanat.

Notă
Numai fișierele / directoarele adăugate de utilizator pot fi șterse,nu și cele care au fost "văzute" automat de BitDefender.

În afară de aceste butoane, există o serie de opțiuni care vă permit să selectați rapid locațiile de scanare.

- **Discuri locale** - pentru scanarea partițiilor locale.
- **Discuri din rețea** - pentru scanarea partițiilor din rețea recunoscute.
- **Unități detașabile** - pentru scanarea unităților mobile de disc (unitățile de CD-ROM și discheta).
- **Toate obiectele** - pentru scanarea tuturor partițiilor, indiferent dacă sunt locale sau de rețea, precum și a unităților detașabile.

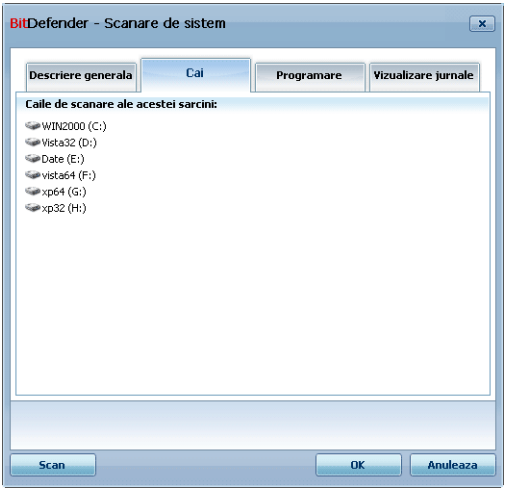
Notă
Dacă doriți să vă scanați tot sistemul, selectați opțiunea **Toate obiectele**.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra. Pentru a executa sarcina faceți clic pe **Scanează**.

Verificarea căii de scanare a sarcinilor de sistem

Nu puteți modifica ținta de scanare pentru sarcinile din categoria **Sarcini sistem**. Puteți doar să vedeți obiectele care vor fi scanate.

Pentru a seta ținta unei anumite sarcini de scanare de sistem, faceți clic-dreapta pe sarcină și selectați **Căi**. de exmplu, pentru sarcina **Scanare de sistem** va apărea următoarea fereastră:



Ținta sarcinii de scanare a sistemului

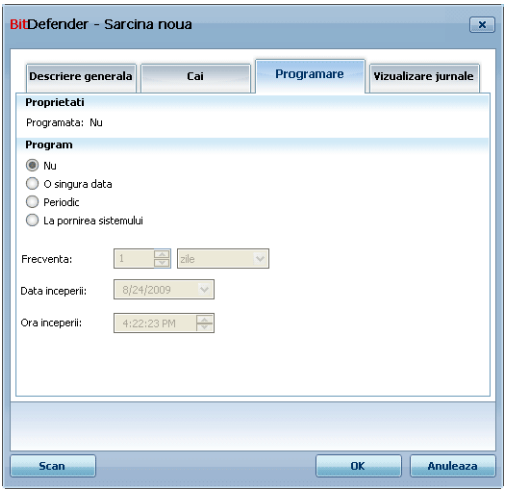
Sarcinile **Scanare de sistem** și **Scanare profundă de sistem** scanează toate partițiile locale, în timp ce sarcina **Scanare rapidă de sistem** scanează doar directoarele `Windows` și `Program Files`.

Faceți clic pe **OK** pentru a închide fereastra. Pentru a executa această sarcină, faceți clic pe **Scanează**.

Planificarea sarcinilor de scanare

Pentru sarcini complexe procesul de scanare durează mai mult și este mai eficient dacă închideți toate programele. Din acest motiv este bine să programați astfel de sarcini să ruleze atunci când nu utilizați sistemul.

Pentru a vizualiza sau modifica programul ueni sarcini, faceți clic-drepata pe sarcină și selectați **Program**. Dacă sunteți deja în fereastra de Proprietăți a sarcinii, selectați tabul **Programare**. Va apărea următoarea fereastră:



Planificare scanări

Puteți vedea programul de rulare al sarcinii, dacă acesta există.

Când planificați o sarcină trebuie să alegeți una dintre următoarele opțiuni:

- **Nu** - lansează sarcina numai la cererea utilizatorului.
- **O singură dată** - sarcina este executată o singură dată, la un anumit moment. Specificați data și timpul lansării în execuție în câmpurile **Data începerii/Ora începerii**.
- **Periodic** - lansează scanarea periodic, la anumite intervale de timp (minute, ore, zile, săptămâni, luni), începând de la o dată și o oră precizate.

  Dacă doriți ca scanarea să se repete la anumite intervale de timp, selectați opțiunea **Periodic** și introduceți în câmpul de editare **La fiecare** numărul de minute/ore/zile/săptămâni /luni reprezantând frecvența acestui proces. De asemenea, trebuie să specificați data și ora lansării în execuție în câmpurile **Datai/Ora începerii**.
- **La pornirea sistemului** - sarcina este executată la numărul de minute specificat după ce un utilizator s-a conectat la Windows.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra. Pentru a executa sarcina faceți clic pe **Scanează**.

18.2.5. Scanarea fișierelor și directoarelor

Înainte de a începe scanarea, este necesar să vă asigurați că BitDefender este la zi cu semnăturile de aplicații malițioase. Scanarea calculatorului folosind semnături vechi poate împiedica BitDefender să detecteze noi aplicații malițioase descoperite după ultima actualizare efectuată. Pentru a vedea când a fost realizată ultima actualizare, faceți clic pe **Actualizare>Actualizare** în modul avansat.

Notă

Pentru ca BitDefender să facă o scanare completă, este necesar să închideți toate programele. Este important să închideți în primul rând clientul de e-mail (i.e. Outlook, Outlook Express sau Eudora).

Sugestii pentru scanare

Iată alte câteva sugestii pentru scanare pe care le-ați putea găsi utile:

- În funcție de dimensiunea hard-discului, scanarea completă a calculatorului (Scanare profundă de sistem sau Scanare de sistem) poate dura (până la o oră sau chiar mai mult). Prin urmare, este recomandat să efectuați astfel de scanări când nu aveți nevoie de calculator pentru mai mult timp (de exemplu, în timpul nopții).

  Puteți programa scanarea să înceapă atunci când este convenabil. Nu uitați să lăsați calculatorul pornit. Pentru Windows Vista, asigurați-vă să nu fie calculatorul în modul de veghe (sleep mode) atunci când sarcina este programată să înceapă.

- Dacă descărcați în mod frecvent fișiere de pe Internet într-un anumit director, creați o sarcină nouă de scanare și setați directorul respectiv ca locație de scanare . Programați sarcina să ruleze în fiecare zi sau mai des.

- Un anumit tip de aplicații malițioase modifică setările Windows pentru a fi lansate automat la pornirea sistemului. Pentru a vă proteja calculatorul împotriva unor astfel de aplicații periculoase, puteți programa sarcina **Scanare automată la conectare** să ruleze automat la pornirea sistemului. Vă rugăm să țineți cont că scanarea autologon poate afecta funcționarea sistemului pentru o scurtă perioadă de timp după pornire.

Metode de scanare

BitDefender oferă patru tipuri de scanare la cerere:

- Scanare imediată - când rulați o sarcină de sistem sau definită de dumneavostră.
- Scanare contextuală - faceți clic-dreapta pe un fișier sau pe un director și selectați opțiunea **Scanează cu BitDefender**.
- Scanare drag&drop - când aduceți un fișier sau director deasupra Barei de scanare.
- Scanare manuală - utilizați scanarea manuală BitDefender pentru a selecta direct fișierele și directoarele ce trebuie scanate.

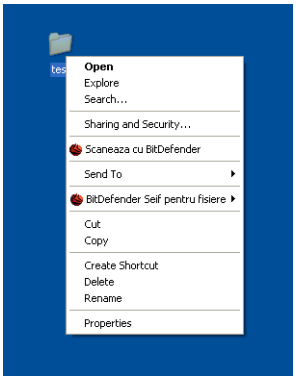
Scanare imediată

Pentru a vă scana sistemul sau o parte din el puteți rula sarcinile de scanare predefinite sau propriile sarcini de scanare. Acest tip de scanare este cunoscut drept scanare imediată.

Pentru a rula o sarcină de scanare a sistemului sau definită de utilizator, faceți clic pe butonul **Rulează sarcina** corespunzător. Va apărea programul asistent de scanare care vă va ghida de-a lungul procesului de scanare.

Scanare contextuală

Pentru a scana un fișier sau un director, fără a mai configura o nouă sarcină de scanare, puteți utiliza meniul contextual. Acest tip de scanare este cunoscut drept scanare contextuală.



Scanare contextuală

Faceți clic-dreapta pe fișierul sau directorul care doriți să fie scanat și selectați opțiunea **Scanează cu BitDefender**. Va apărea programul asistent de scanare care vă va ghida de-a lungul procesului de scanare.

Puteți modifica opțiunile de scanare și examina fișierele de raport accesând fereastra de **Proprietăți** a sarcinii **Scanare meniu contextual**.

Scanare prin drag&drop

Trageți fișierul sau directorul care doriți să fie scanat peste **Bara de scanare**, ca în imaginile de mai jos.

Trageți fișierul

Lăsați fișierul

Va apărea programul asistent de scanare care vă va ghida de-a lungul procesului de scanare.

Scanare manuală

Scanarea manuală constă în selectarea directă a obiectului ce trebuie scanat utilizând opțiunea Scanare manuală BitDefender din grupul BitDefender din meniul Start.

Notă
Scanarea manuală este foarte utilă, mai ales că poate fi realizată și atunci când Windows operează în Safe Mode.

Pentru a selecta obiectul care trebuie scanat de BitDefender, în meniul Windows Start, urmați calea **Start → Programe → BitDefender 2010 → Scanare manuală BitDefender**. Va apărea următoarea fereastră:

Scanare manuală

Faceți clic pe **Adaugă director**, locația care doriți să fie scanată și faceți clic pe **OK**. Dacă doriți să scanați mai multe directoare, repetați această acțiune pentru fiecare locație.

Căile către locațiile selectate vor apărea în coloana **Țintă scanare**. Dacă vă răzgândiți în legătură cu locația, faceți clic pe butonul **Șterge** de lângă aceasta. Faceți clic pe butonul **Elimină toate căile** pentru a elimina toate locațiile care au fost adăugate pe lista.

După ce ați terminat de selectat locațiile, faceți clic pe **Continuă**. Va apărea programul asistent de scanare care vă va ghida de-a lungul procesului de scanare.

Programul asistent de scanare

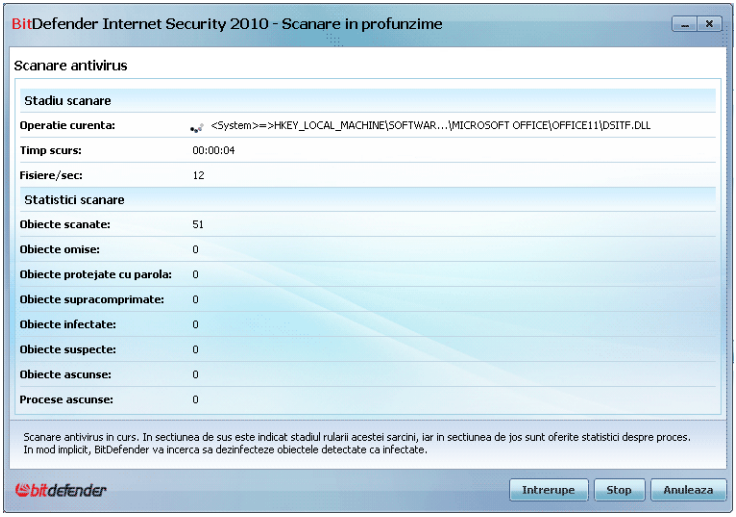
Atunci când inițiați o scanare la cerere, va apărea programul asistent de scanare. Urmați programul asistent în trei pași pentru a realiza procesul de scanare.

Notă

Dacă asistentul de scanare nu apare, este posibil ca scanarea să fie configurată să ruleze discret, în fundal. Căutați iconița de scanare în curs în bara de sistem. Puteți face dublu-clic pe această iconiță pentru a deschide fereastra de scanare și a vedea evoluția scanării.

Pasul 1/3 - Scanare

BitDefender va începe scanarea obiectelor selectate.



Scanare

Puteți vedea stadiul și statisticile scanării (viteza de scanare, timpul scurs de la începutul scanării, numărul obiectelor scanate / infectate / suspecte / ascunse și altele).

Așteptați ca BitDefender să finalizeze scanarea.

Notă
Procesul de scanare poate dura destul de mult, în funcție de complexitatea scanării.

Arhive protejate prin parolă. Dacă BitDefender detectează o arhivă protejată prin parolă în timpul scanării și acțiunea implicită este **Cere parola**, vi se va solicita să furnizați parola. Arhivele protejate prin parolă nu pot fi scanate decât dacă furnizați parola. Următoarele opțiuni sunt disponibile:

- **Parola.** Dacă doriți ca BitDefender să scaneze arhiva, selectați această opțiune și introduceți parola. Dacă nu cunoașteți parola, selectați una dintre celelalte opțiuni.
- **Nu cere parola și omite acest obiect de la scanare.** Selectând această opțiune, arhiva nu fi scanată.

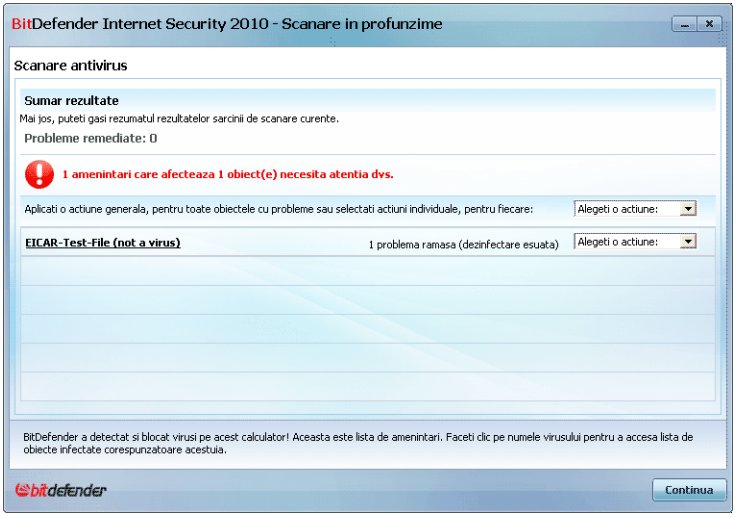
- **Nu scana niciun obiect protejat cu parola.** Selectați această opțiune dacă doriți să nu vi se mai solicite introducerea parolei pentru arhivele protejate prin parolă. BitDefender nu le va putea scana, dar va păstra o înregistrare în raportul de scanare.

Faceți clic pe **OK** pentru a continua scanarea.

Oprirea sau întreruperea temporară a scanării. Puteți opri scanarea oricând doriți făcând clic pe **Stop&Da**. Veți sări direct la ultimul pas al programului asistent. Pentru a opri temporar procesul de scanare, faceți clic pe **Întrerupe**. Va trebui să faceți clic pe **Reia** pentru a relua scanarea.

Pasul 2/3 - Selectați acțiunile

După ce scanarea a fost finalizată, va apărea o nouă fereastră, unde puteți vedea rezultatele scanării.



Acțiuni

Puteți vedea numărul problemelor care vă afectează sistemul.

Obiectele infectate sunt afișate în grupuri, în funcție de codul malware cu care sunt infectate. Faceți clic pe linkul corespunzător unei amenințări pentru a afla mai multe informații despre obiectele infectate.

Puteți alege o acțiune globală care să fie luată asupra tuturor problemelor sau puteți alege acțiuni separate pentru fiecare grup de probleme.

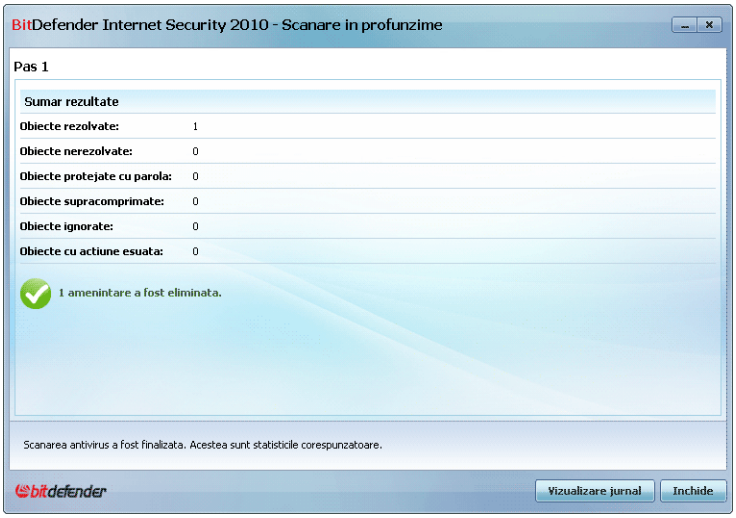
Una sau mai multe dintre opțiunile următoare pot apărea în meniu:

Acțiune	Descriere
Nicio acțiune	Nu se va lua nicio acțiune asupra fișierelor detectate. După finalizarea scanării, puteți deschide raportul de scanare pentru a vedea informații despre aceste fișiere.
Dezinfectează	Elimină codul malițios din fișierele infectate.
Șterge	Șterge fișierele detectate.
Mută în carantină	Mută fișierele detectate în carantină. Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.
Redenumește	Redenumește fișierele ascunse adăugând extensia `.bd.ren` la numele acestora. Ca urmare, veți putea căuta și găsi astfel de fișiere pe calculatorul dumneavoastră, dacă există. Aceste fișiere ascunse nu sunt fișierele pe care le ascundeți deliberat din Windows. Ele sunt fișiere ascunse cu ajutorul unor programe speciale, cunoscute sub numele de rootkituri. Rootkiturile nu sunt în sine programe malițioase. Totuși, ele sunt utilizate frecvent pentru a împiedica detectarea virușilor sau aplicațiilor spion de către programele antivirus obișnuite.

Faceți clic pe **Continuă** pentru a aplica acțiunile specificate.

Pasul 3/3 - Examinați rezultatele

Atunci când BitDefender a remediat toate problemele apărute, rezultatele scanării vor fi afișate într-o nouă fereastră.



Rezumat

Puteți vedea un rezumat al rezultatelor. Dacă doriți informații complete cu privire la procesul de scanare, faceți clic pe **Jurnal** pentru a vizualiza jurnalul de scanare.

Important
Dacă este necesar, reporniți sistemul pentru a finaliza procesul de curățare.

Faceți clic pe **Închide** pentru a închide fereastra.

BitDefender nu a putut remedia anumite probleme

În majoritatea cazurilor, BitDefender va dezinfecta fișierele infectate detectate sau va izola infecția. Cu toate acestea, există anumite probleme care nu pot fi rezolvate.

În aceste cazuri, vă recomandăm să contactați echipa de suport a BitDefender pe pagina web www.bitdefender.ro. Reprezentanții noștri de suport tehnic vă vor ajuta să rezolvați problemele cu care vă confruntați.

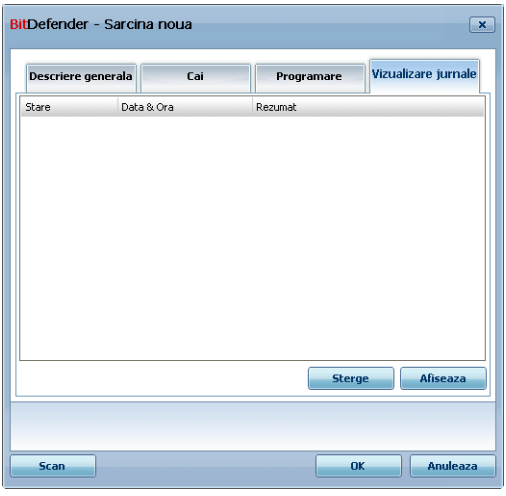
BitDefender a detectat fișiere suspecte

Fișierele suspecte sunt fișiere detectate în cadrul analizei euristice ca fiind posibil infectate cu malware a cărui semnătură nu a fost încă lansată.

Dacă au fost detectate fișiere suspecte în timpul scanării, vi se va cere să le trimiteți laboratorului BitDefender. Faceți clic pe **OK** pentru a trimite aceste fișiere Laboratorului BitDefender spre a fi analizate.

18.2.6. Examinarea rapoartelor de scanare

Pentru a examina rezultatele scanării după rularea unei sarcini, faceți clic-dreapta pe sarcină și selectați **Rapoarte**. Va apărea următoarea fereastră:



Rapoarte

Aici puteți examina rapoartele generate de fiecare dată când sarcina a fost executată. Pentru fiecare fișier sunt oferite informații privind situația procesului de scanare, data și timpul la care a fost executată scanarea precum și un scurt rezumat al rezultatelor scanării.

Sunt disponibile două butoane:

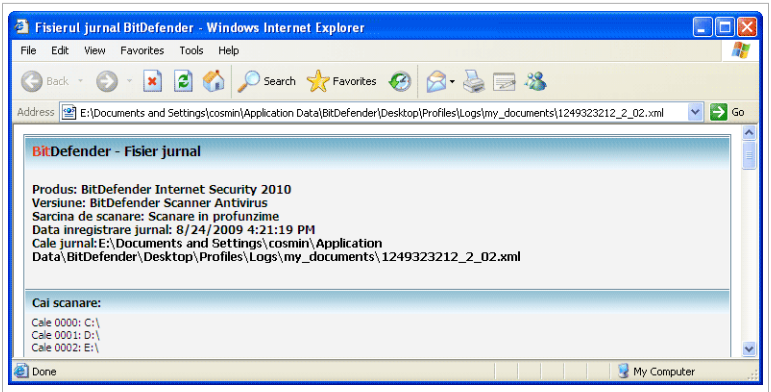
- **Șterge** - șterge fișierul de raport selectat.
- **Afișează** - deschide fișierul de raport selectat. Raportul de scanare va fi deschis în browserul dumneavoastră implicit.

Notă
De asemenea, pentru a deschide sau șterge un fișier de raport, faceți clic-dreapta pe fișier și selectați opțiunea corespunzătoare din meniu.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra. Pentru a executa sarcina faceți clic pe **Scanează**.

Exemplu raport de scanare

Imaginea următoare reprezintă un exemplu de raport de scanare:



Exemplu raport de scanare

Raportul de scanare conține informații detaliate despre procesul de scanare înregistrat, cum ar fi opțiunile de scanare, locațiile scanate, amenințările găsite și acțiunile luate asupra acestor amenințări.

18.3. Obiecte excluse de la scanare

Este posibil ca uneori să fie nevoie să excludeți unele fișiere de la scanare. De exemplu, puteți exclude un fișier de test EICAR de la scanarea la acces sau fișiere `.avi` de la scanarea la cerere.

BitDefender permite excluderea obiectelor atât de la scanarea la acces, cât și de la scanarea la cerere. Această caracteristică este menită să reducă timpul de scanare și să evite orice fel de interferență cu munca dumneavostră.

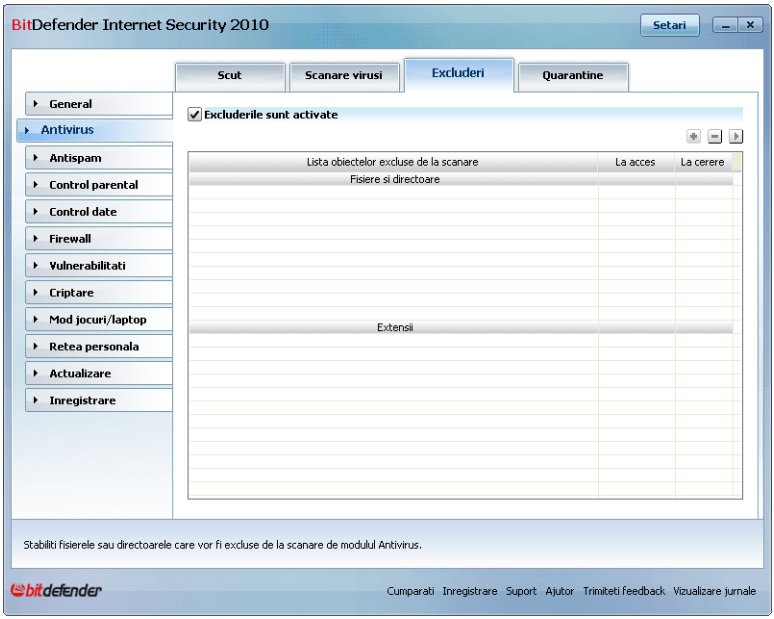
Pot fi excluse de la scanare două tipuri de obiecte:

- **Căi** - fișierul sau directorul (incluzând toate obiectele conținute) indicat de o cale specificată va fi exclus de la scanare.
- **Extensii** - toate fișierele având o extensie specificată vor fi excluse de la scanare.

Notă

Obiectele excluse de la scanarea la acces nu vor fi scanate, indiferent dacă acestea sunt accesate de către dumneavoastră sau de către o aplicație.

Pentru a vedea și administra obiectele excluse de la scanare, mergeți la **Antivirus>Excepții** în Modul Expert.



Excepții

Puteți vedea obiectele (fișiere, directoare, extensii) care sunt excluse de la scanare. Pentru fiecare obiect, puteți vedea dacă este exclus de la scanarea la acces, de la scanarea la cerere sau de la ambele.

Notă

Excepțiile specificate aici NU se vor aplica scanării contextuale. Scanarea contextuală este o metodă de scanare la cerere: faceți clic-dreapta pe fișierul sau directorul pe care doriți să-l scanați și selectați **Scanează cu BitDefender** .

Pentru a șterge un obiect din listă, selectați-l și faceți clic pe butonul **Șterge**.

Pentru a edita un obiect din listă, selectați-l și faceți clic pe butonul **Editează**. Va apărea o nouă fereastră unde puteți schimba extensia sau calea care va fi exclusă, precum și tipul de scanare de la care acestea să fie excluse. Faceți modificările necesare și apoi faceți clic pe **OK**.

Notă

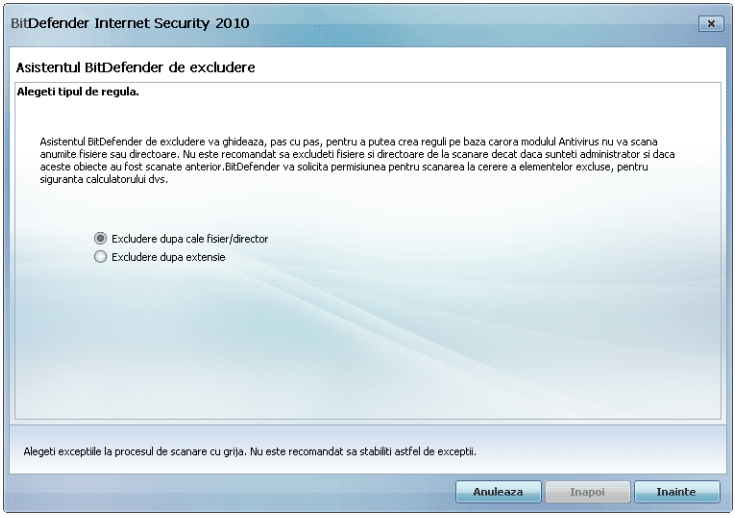
De asemenea, puteți face clic-dreapta pe un obiect și utiliza opțiunile meniului contextual pentru a-l edita sau șterge.

Puteți face clic pe **Revino** pentru a reveni asupra schimbărilor făcute în tabelul de reguli, cu condiția să nu le fi salvat anterior facând clic pe **Aplică**.

18.3.1. Excluderea căilor de la scanare

Pentru a exclude căi de la scanare, faceți clic pe butonul **Adaugă**. Veți fi ghidat pe parcursul procesului de excludere a căilor de la scanare de către programul asistent de configurare care va apărea.

Pasul 1/4 - Selectați tipul obiectului

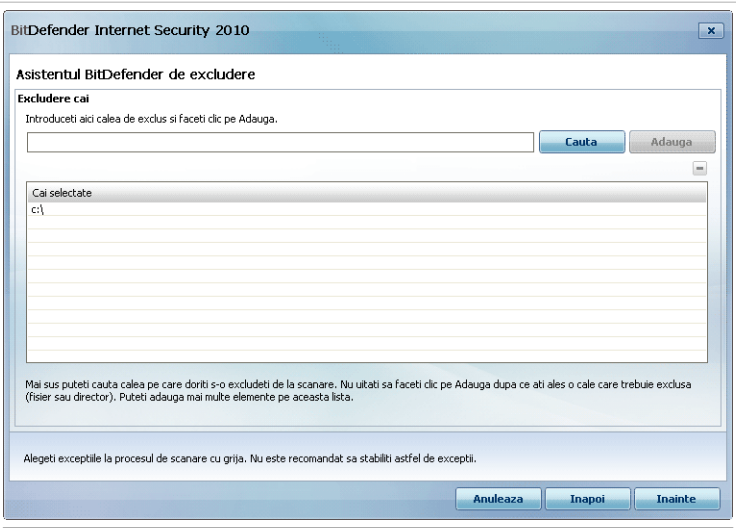


Tip obiect

Selectați opțiunea de excludere a unei căi de la scanare.

Faceți clic pe **Înainte**.

Pasul 2/4 - Specificați căile excluse



Căi excluse

Pentru a preciza căile ce vor fi excluse de la scanare, utilizați una dintre următoarele metode:

- Faceți clic pe **Caută**, selectați fișierul sau directorul care doriți să fie exclus de la scanare și faceți clic pe **Adaugă**.
- Introduceți calea care doriți să fie exclusă de la scanare și faceți clic pe **Adaugă**.

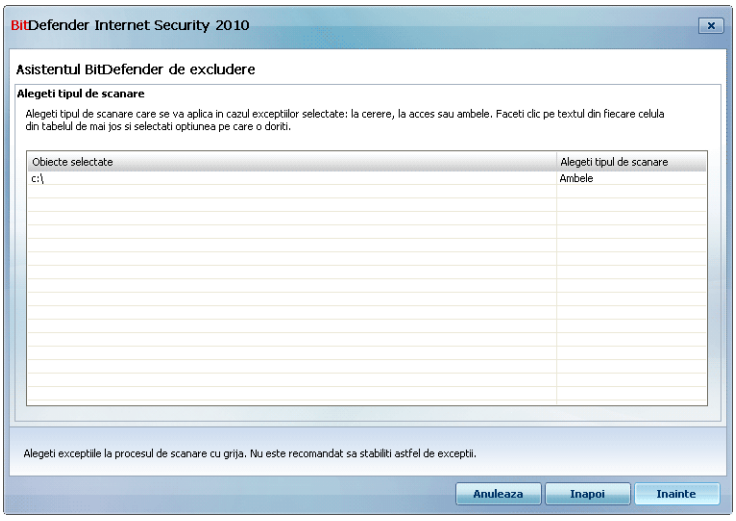
Notă
Un mesaj de eroare va apărea dacă nu există calea furnizată. Faceți clic pe **OK** și verificați validitatea căii.

Căile vor apărea în tabel pe măsură ce le adăugați. Puteți adăuga oricâte căi doriți.

Pentru a șterge un obiect din listă, selectați-l și faceți clic pe butonul **Șterge**.

Faceți clic pe **Înainte**.

Pasul 3/4 - Selectați tipul de scanare



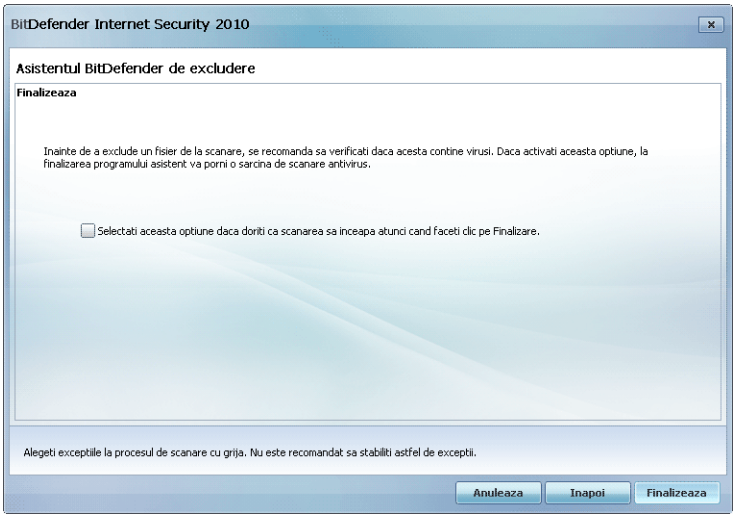
Tip scanare

Puteți vedea un tabel conținând căile ce vor fi excluse de la scanare și tipul de scanare de la care acestea sunt excluse.

Implicit, căile selectate sunt excluse atât de la scanarea la acces cât și de la scanarea la cerere. Pentru a alege când să fie aplicată excepția, faceți clic pe coloana din dreapta și selectați opțiunea dorită din listă.

Faceți clic pe **Înainte**.

Pasul 4/4 - Scanați fișierele excluse



Scanați fișierele excluse

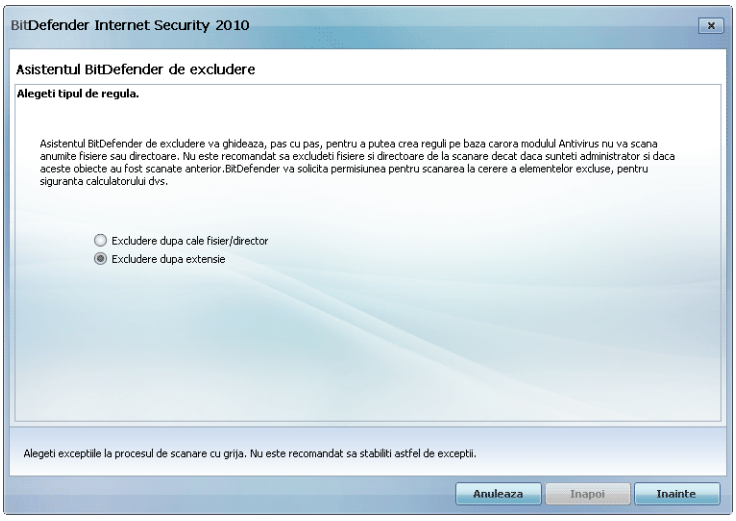
Este recomandat să scanați fișierele din locațiile specificate pentru a vă asigura că acestea nu sunt infectate. Selectați căsuța pentru a scana aceste fișiere înainte de a le exclude de la scanare.

Faceți clic pe **Finalizare**.

18.3.2. Excluderea extensiilor de la scanare

Pentru a exclude extensii de la scanare, faceți clic pe butonul **Adaugă**. Veți fi ghidat pe parcursul procesului de excludere a extensiilor de la scanare de către programul asistent de configurare care va apărea.

Pasul 1/4 - Selectați tipul obiectului

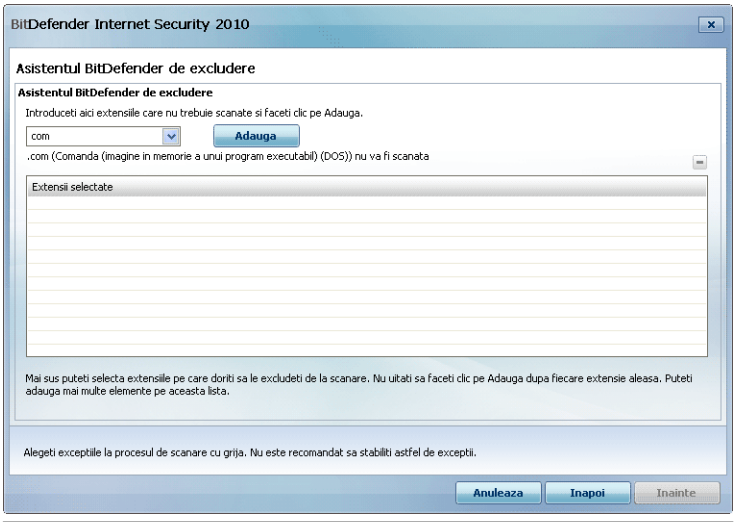


Tip obiect

Selectați opțiunea de excludere a extensiilor de la scanare.

Faceți clic pe **Înainte**.

Pasul 2/4 - Specificați extensiile excluse



Extensii excluse

Pentru a specifica extensiile ce vor fi excluse de la scanare, utilizați una dintre următoarele metode:

- Selectați din meniu extensia care doriți să fie exclusă de la scanare și faceți clic pe **Adaugă**.

> **Notă**
> Meniul conține lista tuturor extensiilor înregistrate pe sistemul dumneavoastră. Atunci când selectați o extensie, îi puteți vedea descrierea, dacă aceasta există.

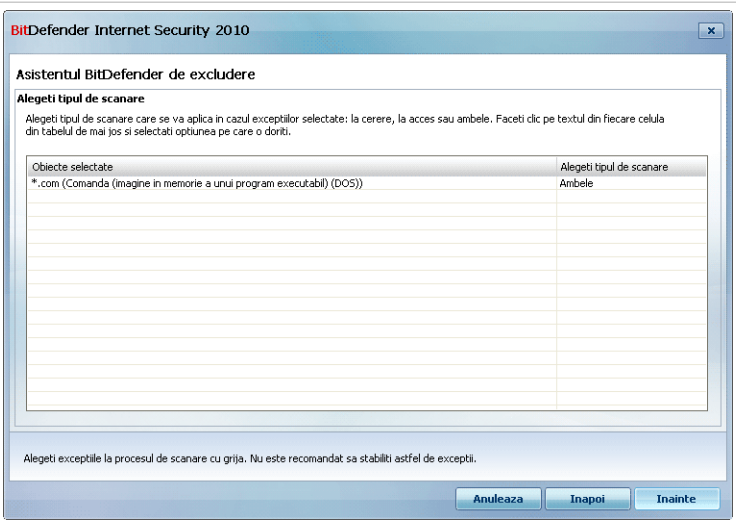
- Introduceți extensia care doriți să fie exclusă de la scanare și faceți clic pe **Adaugă**.

Extensiile vor apărea în tabel pe măsură ce le adăugați. Puteți adăuga oricâte extensii doriți.

Pentru a șterge un obiect din listă, selectați-l și faceți clic pe butonul **Șterge**.

Faceți clic pe **Înainte**.

Pasul 3/4 - Selectați tipul de scanare



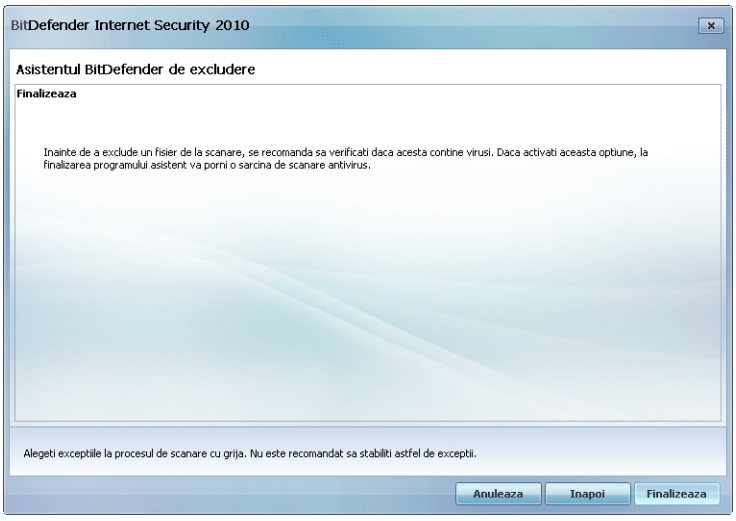
Tip scanare

Puteți vedea un tabel conținând extensiile excluse de la scanare și tipul de scanare de la care acestea sunt excluse.

Implicit, extensiile selectate sunt excluse atât de la scanarea la acces cât și de la scanarea la cerere. Pentru a schimba când să fie aplicată excepția, faceți clic pe coloana din dreapta și selectați opțiunea dorită din listă.

Faceți clic pe **Înainte**.

Pasul 4/4 - Selectați tipul de scanare



Tip scanare

Este recomandat să scanați fișierele care au extensiile specificate pentru a vă asigura că acestea nu sunt infectate.

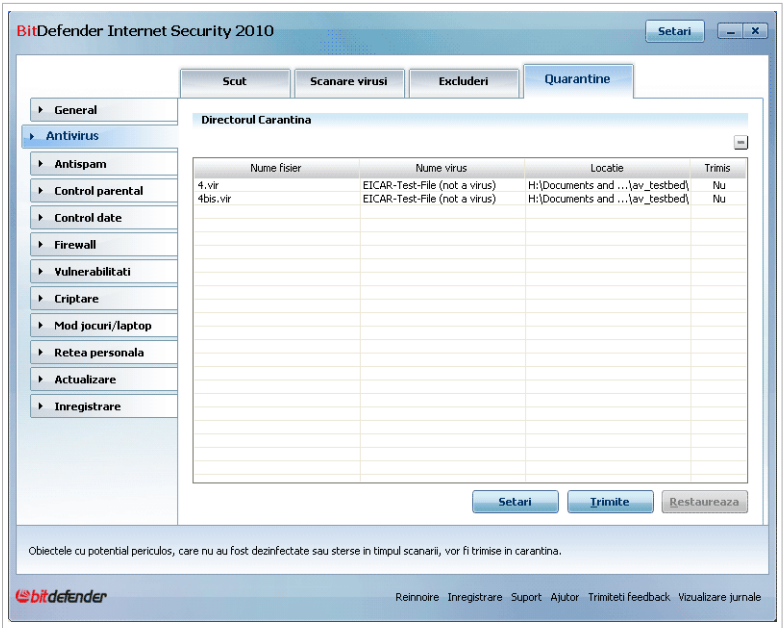
Faceți clic pe **Finalizare**.

18.4. Zona de carantină

BitDefender permite izolarea fișierelor infectate sau suspecte într-o zonă sigură, numită carantină. Izolând aceste fișiere în carantină, riscul răspândirii infecției dispare, iar în plus, aveți posibilitatea să trimiteți aceste fișiere Laboratorului BitDefender pentru analiză aprofundată.

În plus, BitDefender scanează fișierele din carantină după fiecare actualizare a semnăturilor de aplicații malițioase. Fișierele curățate sunt mutate automat în locația lor originală.

Pentru a vedea și administra fișierele din carantină și pentru a configura setările carantinei, mergeți la **Antivirus>Carantină** în Modul Expert.



Carantinează

Secțiunea Carantină afișează toate fișierele izolate în directorul Carantină. Puteți vedea numele fiecărui fișier, numele virusului detectat, calea către locația originală și data trimiterii.

Notă
Atunci când sunt în carantină virușii sunt inofensivi, pentru că nu pot fi executați sau citiți.

18.4.1. Gestionarea fișierelor din carantină

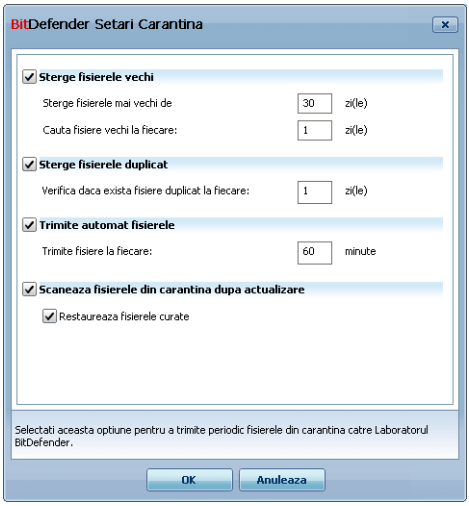
Puteți trimite fișierele selectate la Laboratorul BitDefender pentru o analiză detaliată facând clic pe **Trimite**. Implicit, BitDefender va trimite automat fișierele din carantină la fiecare 60 minute.

Pentru a șterge un fișier selectat din carantină faceți clic pe butonul **Șterge**. Dacă doriți să mutați fișierul selectat în locația inițială, faceți clic pe **Restaurează**.

Meniul contextual. Un meniu contextual este disponibil, permițând gestionarea rapidă a fișierelor din carantină. Aceleași opțiuni ca cele amintite anterior sunt disponibile. De asemenea, puteți selecta **Actualizează** pentru a actualiza carantina.

18.4.2. Configurarea setărilor carantinei

Pentru a configura setările carantinei, faceți clic pe **Setări**. Va apărea o nouă fereastră.



Setări Carantină

Utilizând setările carantinei, puteți seta BitDefender să execute automat următoarele acțiuni:

Șterge fișierele vechi. Pentru a șterge automat fișierele vechi din carantină, bifați opțiunea corespunzătoare. Trebuie să specificați numărul de zile după care fișierele din carantină ar trebui șterse și frecvența cu care BitDefender să caute fișiere vechi.

Notă
Implicit, BitDefender va căuta fișiere vechi în fiecare zi și va șterge fișierele mai vechi de 30 de zile.

Șterge fișierele duplicat. Pentru a șterge automat fișierele duplicat din carantină, bifați opțiunea corespunzătoare. Trebuie să specificați numărul de zile dintre două căutări consecutive de fișiere duplicat.

Notă
Implicit, BitDefender va căuta fișiere duplicat în carantină în fiecare zi.

Trimite automat fișierele. Pentru a trimite automat fișierele din carantină, bifați opțiunea corespunzătoare. Trebuie să specificați frecvența cu care să fie trimise fișierele.

Notă
Implicit, BitDefender va trimite automat fișierele din carantină la fiecare 60 minute.

Scanează fișierele din carantină după actualizare. Pentru a scana automat fișierele aflate în carantină după fiecare actualizare, bifați opțiunea corespunzătoare. Puteți muta automat fișierele curățate în locația originală selectând **Restaurează fișiere curățate**.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

19. Antispam

BitDefender Antispam utlizează remarcabile inovații tehnologice și filtre antispam standard pentru a ține la distanță spamul de căsuțele de mesaje ale utilizatorilor.

19.1. Detalii privind modulul Antispam

Spam-ul este o problemă în creștere, atât pentru individ cât și pentru organizații. Nu este interesant, nu ați dori să fie văzut de către copii, puteți fi concediat din cauza lui (pentru pierdere de timp prin primirea de mesaje cu conținut sexual pe adresa de serviciu) și nu puteți împiedica trimiterea sa. Cel mai bun lucru pe care îl puteți face este, evident, să nu îl mai primiți. Din păcate, acesta există în cantități mari, într-o gamă largă de forme și mărimi.

19.1.1. Filtrele Antispam

Motorul BitDefender Antispam incorporează șapte filtre diferite care vă protejează directorul Inbox de Spam:Lista de prieteni, Lista de spammeri, Filtrul de caractere, Filtrul de imagini, Filtrul URL, Filtrul NeuNet(euristic) și Filtrul Bayesian.

Notă

Puteți activa / dezactiva fiecare dintre aceste filtre în secțiunea Setări din modulul **Antispam**.

Lista de prieteni / spammeri

Majoritatea oamenilor comunică în mod regulat cu un grup de cunoștințe sau chiar primesc mesaje de la companii sau organizații cu același domeniu de activitate. Folosind **listele de prieteni și spammeri** îi puteți clasifica ușor pe cei de la care doriți să primiți mesaje (prieteni), indiferent de conținut, sau cei de la care nu doriți să primiți nimic (spammeri).

Listele de prieteni / spammeri pot fi administrate din Modul Expert sau din bara de comenzi Antispam integrată în unii dintre cel mai des folosiți clienți de mail.

Notă

Vă recomandăm să adăugați numele și adresele prietenilor la **lista de prieteni**.BitDefender nu va bloca mesajele de la cei de pe listă; deci adăugând prietenii vă veți asigura că mesajele legitime vor ajunge în Inbox.

Filtrul de caractere

Multe mesaje Spam sunt scrise cu caractere chirilice și / sau asiatice. Filtrul de caractere detectează acest tip de mesaje și le marchează ca SPAM.

Filtrul de imagini

Pentru că evitarea filtrului euristic a devenit o provocare, în ultima vreme, directoarele inbox sunt invadate de mesaje spam ce au o singură imagine atașată. Pentru rezolvarea acestei probleme crescânde, BitDefender a introdus**Image filter**, care compară semnăturile imaginilor din mesaje cu cele dintr-o bază de date a BitDefender. Dacă se descoperă o imagine cu conținut spam mesajul va fi marcat ca SPAM.

Filtrul URL

Aproape toate mesajele spam conțin referințe (linkuri) la diverse pagini web. Aceste pagini conțin, de obicei, reclame și oferă posibilitatea de a cumpăra obiecte și, uneori, sunt folosite pentru tentative de phishing.

BitDefender menține o bază de date cu astfel de linkuri. Filtrul URL caută fiecare link URL dintr-un mesaj în baza sa de date. Dacă linkul este găsit, mesajul este marcat ca SPAM.

Filtrul Euristic

Filtrul NeuNet (euristic) verifică toate componentele unui mesaj, (nu doar header-ul, dar și corpul mesajului în format HTML sau text), căutând cuvinte, fraze, linkuri sau alte caracteristici ale spamului. Pe baza rezultatelor analizei, filtrul adaugă un scor SPAM mesajului.

Filtrul detectează, de asemenea, mesajele marcate `SEXUALLY-EXPLICIT:` în subiect și le marchează ca SPAM.

Notă

Începând din 19 Mai 2004, mesajele Spam care conțin material cu specific sexual trebuie să includă avertismentul `SEXUALLY-EXPLICIT:` în subiect. În caz contrar expeditorii vor fi acuzați de încălcarea legii și ulterior amendați.

Filtrul Bayesian

Filtrul Bayesian verifică mesajele ținând cont de informații statistice despre frecvența cu care anumite cuvinte apar în mesaje clasificate ca Spam comparativ cu mesajele non-Spam (vor fi folosite mesajele etichetate de dumneavoastră sau de către Filtrul Euristic).

Aceasta înseamnă că, dacă filtrul observă că un anumit cuvânt format din patru litere apare mai des în mesajele Spam, acesta va presupune că există o probabilitate ridicată ca următorul mesaj ce conține respectivul cuvânt să fie Spam. Toate cuvintele semnificative din mesaje sunt verificate. Sintetizând informațiile statistice, se calculează probabilitatea ca un anumit mesaj să fie Spam.

Acest modul prezintă o altă caracteristică interesantă: este educabil. Se adaptează rapid la tipul de mesaje primite de un anumit utilizator și stochează informații cu

privire la toate mesajele. Pentru a funcționa eficient, filtrul trebuie educat, adică trebuie să i se dea exemple de Spam precum și de mesaje legitime, la fel cum unui câine i se indică mirosul pe care trebuie să îl găsească. Uneori filtrul trebuie să fie și corectat / atenționat atunci când clasifică greșit unele mesaje.

Important

Puteți corecta filtrul Bayesian folosind butoanele **Este Spam** și **Nu este Spam** din bara de comenzi Antispam.

19.1.2. Funcționarea modulului Antispam

Motorul antispam al BitDefender utilizează concomitent toate filtrele antispam pentru a determina dacă un anumit mesaj e-mail ar trebui să ajungă în directorul **Inbox (Mesaje primite)** sau nu.

Important

Mesajele spam detectate de BitDefender sunt marcate cu prefixul [SPAM] în subiect. BitDefender mută în mod automat mesajele spam într-un anumit director, după cum urmează:

- În Microsoft Outlook, mesajele spam sunt mutate într-un director **Spam**, situat în directorul **Deleted Items**. Directorul **Spam** este creat în timpul instalării BitDefender.
- În Outlook Express și Windows Mail, mesajele spam sunt mutate direct în **Deleted Items**.
- În Mozilla Thunderbird, mesajele spam sunt mutate într-un director **Spam**, situat în directorul **Trash**. Directorul **Spam** este creat în timpul instalării BitDefender.

Dacă utilizați alt client de mail, trebuie să creați o regulă pentru a muta mesajele e-mail marcate [SPAM] de BitDefender într-un anumit director de carantină.

Fiecare mesaj e-mail pe care îl primiți este întâi verificat de filtrul Lista de prieteni/Lista de spammeri. Dacă adresa expeditorului se regăsește în Lista de prieteni mesajul este trimis direct în **Inbox**.

În caz contrar, filtrul Lista de spammeri va verifica dacă adresa expeditorului se află pe această listă. Dacă adresa se regăsește pe lista neagră, mesajul este etichetat ca SPAM și este mutat în directorul **Spam** (localizat în Microsoft Outlook).

Altfel, Filtrul de caractere va verifica dacă mesajul este scris cu caractere Chirilice sau Asiatice. Dacă mesajul este scris astfel, el va fi etichetat ca SPAM și mutat în directorul **Spam**.

Dacă mesajul nu este scris cu caractere asiatice sau chirilice, acesta va fi transmis Filtrului de imagini. **Filtrul de imagini** va detecta toate mesajele e-mail care au atașate imagini cu conținut spam.

Filtrul URL va căuta link-uri și va compara link-urile găsite cu link-urile din baza de date BitDefender. În cazul în care un link din mesaj este găsit în baza de date, mesajul va primi un scor Spam.

Filtrul NeuNet(euristic) va prelua mesajul și va verifica toate componentele acestuia, căutând cuvinte, fraze, linkuri sau alte caracteristici spam. Și în acest caz, mesajul va primi un scor Spam.

Notă
Dacă mesajul este etichetat ca SEXUALLY EXPLICIT în subiect, BitDefender îl va considera SPAM.

Filtrul Bayesianva analiza mesajul în continuare, ținând cont de informații statistice despre frecvența cu care anumite cuvinte apar în mesaje clasificate ca Spam comparativ cu mesajele non-Spam (vor fi folosite mesajele etichetate de dumneavoastră sau de către Filtrul Euristic). Mesajul va primi un alt scor Spam.

Dacă scorul Spam însumat (scorul URL + scorul Euristic + scorul Bayesian) depășește scorul Spam pentru un mesaj (setat de către utilizator în secțiunea Antispam ca nivel de toleranță), mesajul este considerat SPAM.

19.1.3. Actualizări Antispam

La fiecare actualizare:

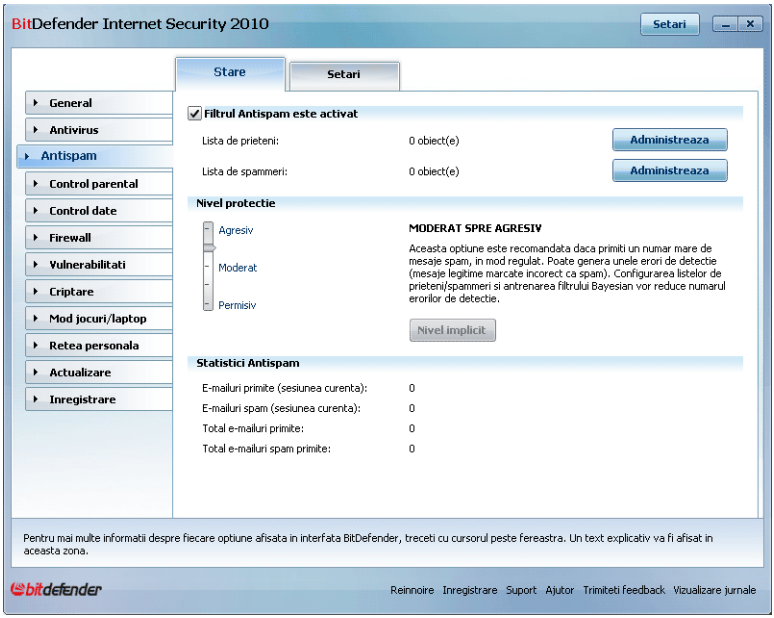
- noi semnături de imagini vor fi adăugate **Filtrului de imagini**.
- noi linkuri vor fi adăugate **Filtrului URL**.
- noi reguli vor fi adăugate **Filtrului NeuNet (euristic)**.

Aceasta permite sporirea eficienței motorului Antispam.

Pentru a vă proteja de spammeri, BitDefender poate realiza actualizări automate. Păstrați opțiunea **Actualizare automatică** activată.

19.2. Stare

Pentru a configura protecția Antispam, mergeți la **Antispam>Stare** în Modul Expert.



Status Antispam

Puteți vedea dacă filtrul Antispam este activat sau nu. Pentru a schimba starea filtrului Antispam, debifați sau selectați căsuța corespunzătoare.

Important
Pentru a vă proteja directorul**Inbox** de Spam, păstrați **filtrul Antispam**activat.

În secțiunea **Statistici** puteți vedea rezultatele activității antispam pentru fiecare sesiune (de când ați pornit calculatorul) sau un rezumat al acesteia (de la instalarea BitDefender).

19.2.1. Setarea nivelului de protecție

Puteți alege nivelul de protecție adecvat nevoilor dumneavoastră de securitate. Mutați cursorul pentru a seta nivelul de protecție dorit.

Există cinci niveluri de protecție:

Nivel de protecție	Descriere
Permisiv	Oferă protecție pentru conturi de mail ce primesc foarte multe mesaje comerciale legitime. Filtrul va lăsa majoritatea mesajelor să treacă, dar se pot produce falsuri negative (spam clasificat ca mesaj legitim).
Permisiv către moderat	Oferă protecție pentru conturi de mail ce primesc unele mesaje comerciale legitime. Filtrul va lăsa majoritatea mesajelor să treacă, dar se pot produce falsuri negative (spam clasificat ca mesaj legitim).
Moderat	Oferă protecție pentru conturi de mail obișnuite. Filtrul va bloca majoritatea mesajelor spam, evitând falsurile pozitive.
Moderat către agresiv	Oferă protecție pentru conturi de mail ce primesc volume mari de spam în mod regulat. Filtrul va lăsa foarte puțin spam să treacă, dar se pot produce falsuri pozitive (mesaje legitime incorect marcate ca spam). Configurați **Listele de prieteni/spammeri** si antrenați **Motorul de învățare (Bayesian)** pentru a reduce numărul falsurilor pozitive.
Agresiv	Oferă protecție pentru conturi de mail ce primesc volume foarte mari de spam în mod regulat. Filtrul va lăsa foarte puțin spam să treacă, dar se pot produce falsuri pozitive (mesaje legitime incorect marcate ca spam). Adăgați-vă contactele la **lista de prieteni** pentru a reduce numărul falsurilor pozitive.

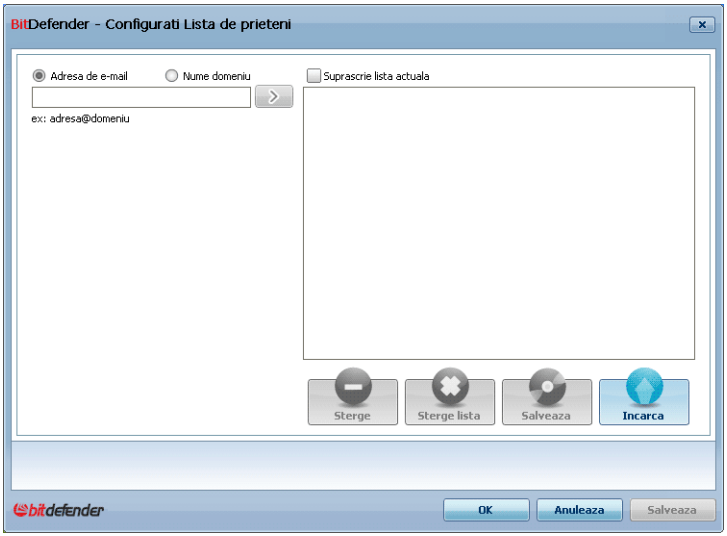
Pentru a seta nivelul implicit de protecție (**Moderat către agresiv**) faceți clic pe **Nivel implicit**.

19.2.2. Configurați lista de prieteni

Lista de prieteni este o listă care conține toate adresele de e-mail de la care doriți să primiți mesaje, indiferent de conținutul acestora. Mesajele de la prieteni nu vor fi etichetate Spam, chiar dacă au conținut asemănător mesajelor Spam.

Notă
Orice mesaj venit de la o adresă inclusă în **lista de prieteni** va fi trimis automat în directorul Inbox, fără a mai fi procesat.

Pentru a configura Lista de prieteni, faceți clic pe **Administrați prieteni** (sau pe butonul **Prieteni** din Bara de comenzi Antispam).



Lista de prieteni

Aici puteți adăuga sau șterge intrări din **lista de prieteni**.

Dacă doriți să adăugați o adresă, selectați **Adresă de e-mail**, scrieți adresa și faceți clic pe butonul . Adresa va apărea pe **Lista de prieteni**.

Important
Sintaxă: name@domain.com.

Dacă doriți să adăugați un domeniu, selectați opțiunea **Domeniul**, scrieți domeniul și faceți clic pe butonul . Domeniul va apărea în **lista de prieteni** .

Important
Sintaxă:

- @domain.com, *domain.com și domain.com - toate mesajele primite de la domain.com vor ajunge în directorul **Inbox** indiferent de conținut;
- *domain* - toate mesajele primite de la domain (indiferent de sufixul domeniului) vor ajunge în directorul **Inbox** indiferent de conținut;
- *com - toate mesajele primite având sufixul domeniului com vor ajunge în directorul **Inbox** indiferent de conținut;

Pentru a șterge un obiect de pe listă, selectați-l și faceți clic pe butonul **Șterge**. Pentru a șterge toate înregistrările de pe listă faceți clic pe butonul **Șterge jurnal** și apoi pe **Da**, pentru confirmare.

Puteți salva Lista de prieteni într-un fișier, astfel încât s-o puteți folosi pe un alt calculator sau după reinstalarea produsului. Pentru a salva Lista de prieteni, faceți clic pe butonul **Salvează** și salvați-o în locația dorită. Fișierul va avea o extensie `.bwl`.

Pentru a încărca o Listă de prieteni salvată anterior, faceți clic pe butonul **Încărca** și deschideți fișierul `.bwl` corespunzător. Pentru a reseta conținutul listei curente atunci când încărcați o listă salvată anterior selectați **Suprascrie lista curentă**.

Notă

Vă recomandăm să adăugați numele și adresele prietenilor la **lista de prieteni**.BitDefender nu va bloca mesajele de la cei de pe listă; deci adăugând prietenii vă veți asigura că mesajele legitime vor ajunge în Inbox.

Faceți clic pe **Salvează** și **OK** pentru a salva modificările și a închide **Lista de prieteni**.

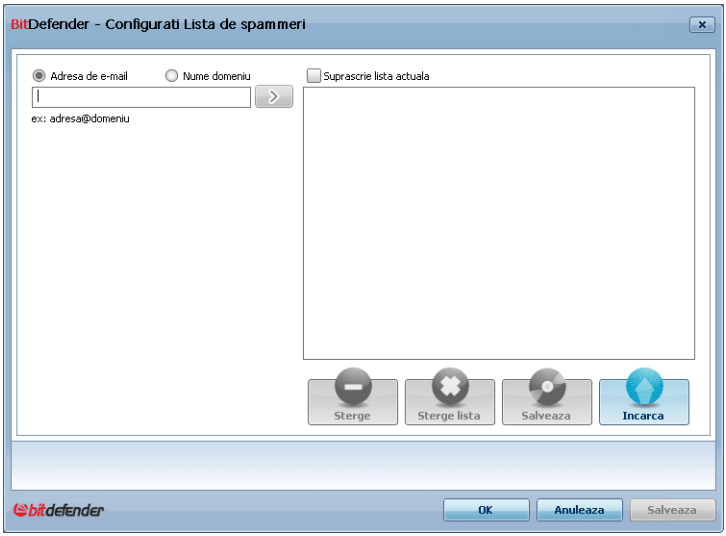
19.2.3. Configurarea listei de spammeri

Lista de spammeri este o listă care conține toate adresele de e-mail de la care nu doriți să primiți mesaje, indiferent de conținutul acestora.

Notă

Orice mesaj primit de la o adresă din **lista de spammeri** va fi automat etichetat ca Spam, fără altă procesare.

Pentru a configura Lista de spammeri, faceți clic pe **Administrați spammeri** (sau pe butonul **Spammeri** din Bara de comenzi Antispam).



Lista de spammeri

Aici puteți adăuga sau șterge intrări din **lista de spammeri** .

Dacă doriți să adăugați o adresă, selectați **E-mail**, scrieți adresa și faceți clic pe butonul . Adresa va apărea în **lista de spammeri**.

Important
Sintaxă: name@domain.com.

Dacă doriți să adăugați un domeniu, selectați **Domeniul**, scrieți domeniul și faceți clic pe butonul . Domeniul va apărea în **lista de spammeri**.

Important
Sintaxă:

- @domain.com, *domain.com and domain.com - - toate mesajele primite de la domain.com vor fi etichetate ca SPAM;
- *domain* - toate mesajele primite de la domain(indiferent de sufixul domeniului) vor fi etichetate ca SPAM;
- *com - a- toate mesajele primite având sufixul domeniului com vor fi etichetate ca SPAM.

Avertisment

Nu adăugați nume de domenii legitime ale unor servicii de e-mail bazate pe web (Yahoo, Gmail, Hotmail sau altele asemenea) pe Lista de spammeri. În caz contrar,

mesajele e-mail primite de la orice utilizator înregistrat al unui astfel de serviciu vor fi detectate ca spam. Dacă, de exemplu, adăugați `yahoo.com` pe Lista de spammeri, toate mesajele e-mail care provin de la adrese `yahoo.com` vor fi marcate ca `[spam]`.

Pentru a șterge un obiect de pe listă, selectați-l și faceți clic pe butonul **Șterge**. Pentru a șterge toate înregistrările de pe listă faceți clic pe butonul **Șterge jurnal** și apoi pe **Da**, pentru confirmare.

Puteți salva Lista de spammeri într-un fișier astfel încât s-o puteți folosi pe un alt calculator sau după reinstalarea produsului. Pentru a salva Lista de spammeri, faceți clic pe butonul **Salvează** și salvați-o în locația dorită. Fișierul va avea o extensie `.bwl`.

Pentru a încărca o Listă de spammeri salvată anterior, faceți clic pe butonul **Încărca** și deschideți fișierul `.bwl` corespunzător. Pentru a reseta conținutul listei curente atunci când încărcați o listă salvată anterior selectați **Suprascrie lista curentă**.

Faceți clic pe **Salvează**și**OK** pentru a salva modificările și a închide **Lista de spammeri**.

Important
Dacă doriți să reinstalați BitDefender este recomandar să salvați listele de **Prieteni** / **Spammeri** înainte, iar după instalare le puteți încărca.

19.3. Setări

Pentru a configura setările și filtrele antispam, mergeți la **Antispam>Setări** în Modul Expert.

Setări Antispam

Sunt disponibile trei categorii de opțiuni (**Setări Antispam**, **Filtre Antispam elementare** și **Filtre Antispam avansate**) organizate într-un meniu expandabil, similar celor din Windows.

Notă
Faceți clic pe semnul “+” pentru a deschide o categorie sau pe “-” pentru a închide categoria.

Pentru a activa/dezactiva un filtru bifați/debifați căsuța corespunzătoare.

Pentru a aplica setările implicite, faceți clic pe **Nivel implicit**.

Faceți clic pe **Aplică** pentru a salva modificările.

19.3.1. Setări Antispam

- **Marchează mesajele cu [spam] în subiect** - toate mesajele considerate spam vor fi marcate cu textul [spam] în subiect.
- **Marcheaza mesajele cu [phishing] în subiect** - toate mesajele considerate phishing vor fi marcate cu textul [phishing] în subiect.

19.3.2. Filtre Antispam elementare

- **Activează Lista de prieteni/spammeri** - filtrează mesajele e-mail folosind Listele de prieteni /spammeri.
  - **Adaugă automat destinatarii pe lista de prieteni** - adăugă automat destinatarii mesajelor trimise pe lista de prieteni.
  - **Adaugă automat pe lista de prieteni** - atunci când faceți clic pe butonul **Nu este spam** din bara de comenzi Antispam expeditorul este adăugat automat pe lista de prieteni.
  - **Adaugă automat pe lista de spammeri** - atunci când faceți clic pe butonul **Este Spam** din bara de comenzi Antispam expeditorul este adăugat automat pe Lista de spammeri.

Notă

Butoanele **Nu este Spam** și **Este Spam** sunt folosite pentru educarea filtrului Bayesian.

- **Blochează mesajele e-mail scrise cu caractere asiatice** - blochează mesajele scrise cu caractere asiatice.
- **Blochează mesajele e-mail scrise cu caractere chirilice** - blochează mesajele scrise cu caractere chirilice.

19.3.3. Filtre Antispam avansate

- **Activează motorul de învățare (Bayesian)** - activează/dezactivează motorul de învățare (Bayesian).
  - **Limitează mărimea dicționarului la 200000 de cuvinte** - setează dimensiunea dicționarului Bayesian - mai mic înseamnă mai rapid, mai mare înseamnă mai eficient.

Notă

Dimensiunea recomandată este de 200.000 de cuvinte.

  - **Antrenează motorul de învățare (Bayesian) cu mesaje trimise** - antrenează motorul de învățare (Bayesian) cu mesajele trimise.
- **Filtrul URL** - activează/dezactivează filtrul URL;
- **Filtrul NeuNet(euristic)** - activează/dezactivează Filtrul NeuNet(euristic).
  - **Blochează conținutul explicit** - activează/dezactivează detectarea mesajelor ce conțin în subiect SEXUALLY EXPLICIT.
- **Filtrul de imagine** - activează/dezactivează Filtrul de imagine.

20. Control parental

Controlul parental BitDefender vă permite să controlați accesul la Internet și la anumite aplicații pentru fiecare utilizator care deține un cont de utilizator pe sistem.

Puteți configura Controlul parental să blocheze:

- pagini web inadecvate.
- accesul la Internet, pentru anumite intervale de timp (de exemplu, în timpul rezervat lecțiilor).
- paginile web, mesajele e-mail și mesajele instant care conțin anumite cuvinte cheie.
- jocuri, aplicații de chat, partajare de fișiere și altele.
- mesaje instant trimise de alte contacte IM decât cele permise.

Important

Doar utilizatorii cu drepturi administrative pe sistem (administratorii de sistem) pot accesa și configura Controlul parental. Pentru a vă asigura că doar dumneavoastră puteți modifica setările de Control parental pentru oricare utilizator, puteți proteja aceste setări cu o parolă. Vi se va cere să configurați parola atunci când activați Controlul parental pentru un anumit utilizator.

Pentru a utiliza eficient Controlul parental pentru restricționarea activităților online și pe calculator ale copiilor dumneavoastră, trebuie să îndepliniți aceste sarcini principale:

1. Creați conturi de utilizator Windows limitate (standard) pentru copiii dumneavoastră.

Notă

Pentru a afla cum să creați conturi de utilizator Windows, consultați Centrul de suport și ajutor al Windows (în meniul Start, faceți clic pe **Help and Support**).

2. Configurați Controlul parental pentru conturile de utilizator folosite de copiii dumneavoastră.

Pentru a configura Controlul parental, mergeți la **Control parental** în Modul Expert.

Control parental

Puteți vedea informații despre starea Controlului Parental, pentru fiecare cont de utilizator Windows. Categoria de vârstă este afișată sub fiecare nume de utilizator dacă este activat Controlul parental. Când Controlul parental este dezactivat, starea sa apare ca **neconfigurat**.

În plus, puteți vedea starea fiecărei caracteristici de Control parental, pentru fiecare utilizator:

Cerc verde cu bifă: Caracteristica este activată.

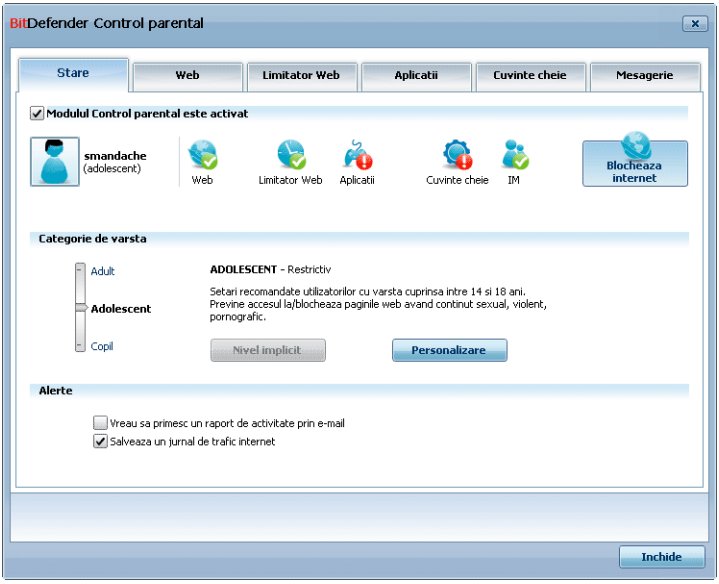
Cerc roșu cu semnul exclamării: Caracteristica este dezactivată.

Faceți clic pe butonul **Modifică** din dreptul unui nume de utilizator pentru a deschide fereastra în care puteți configura setările de Control parental pentru respectivul cont de utilizator.

Următoarele secțiuni din acest capitol prezintă în detaliu caracteristicile de Control parental și cum să le configurați.

20.1. Configurarea Controlului parental pentru un utilizator

Pentru a configura Controlul parental pentru un anumit cont de utilizator, faceți clic pe butonul **Modificare** corespunzător acestuia și apoi pe tabul **Stare**.



Status Control parental

Pentru a configura Controlul parental pentru acest cont de utilizator, urmați acești pași:

1. Activați Controlul parental pentru acest cont de utilizator selectând căsuța **Control parental**.

   Important
   Păstrați **Controlul Parental** activat pentru a vă proteja copiii împotriva conținutului web inadecvat utilizând regulile dumneavoastră privind accesul la calculator.

2. Setați o parolă pentru a proteja setările dumneavoastră de Control parental. Pentru mai multe informații, consultați *„Protejarea setărilor de Control parental”* (p. 192).
3. Setați categoria de vârstă pentru a permite copilului dumneavoastră să acceseze numai site-uri web potrivite pentru vârstă lui. Pentru mai multe informații, consultați *„Setarea categorie de vârstă”* (p. 193).
4. Configurați opțiunile de monitorizare pentru acest utilizator, după cum doriți:
   - **Trimite-mi un raport de activitate prin e-mail.** O notificare prin e-mail este trimisă de fiecare dată când modulul Control Parental al BitDefender blochează o activitate a acestui utilizator.

- **Salvează un jurnal de trafic internet.** Înregistrează în jurnal site-urile web vizitate de utilizator.

Pentru mai multe informații, consultați *„Monitorizarea activității copiilor”* (p. 196).

5. Faceți clic pe o iconiță sau pe un tab pentru a configura corespunzător modulul Control parental:
   - **Web** - pentru a filtra navigarea în rețea conform regulilor stabilite de dumneavoastră în secțiunea Web.
   - **Aplicații** - pentru a bloca accesul la aplicațiile pe care le precizați în secțiunea Aplicații.
   - **Cuvinte cheie** - pentru a filtra accesul la web, mail și mesageria instant conform regulilor stabilite de dumneavoastră în secțiunea Cuvinte cheie.
   - **Mesagerie instant** - pentru a bloca sau permite conversațiile cu utilizatori de mesagerie instant conform regulilor stabilite de dumneavoastră în secțiunea Trafic mesagerie instant.
   - **Limitator de timp** - pentru a permite accesul la rețea conform orarului stabilit de dumneavoastră în secțiunea Limitator de timp.

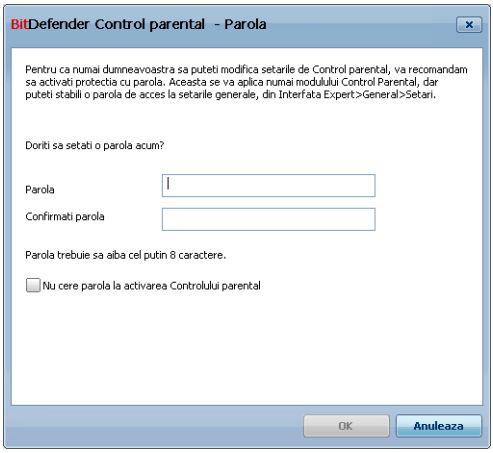
Notă
Pentru a afla cum să le configurați, consultați următoarele secțiuni din acest capitol.

Pentru a bloca complet accesul la Internet, faceți clic pe butonul **Blochează Internet**.

20.1.1. Protejarea setărilor de Control parental

Dacă nu sunteți singura persoană cu drepturi administrative care utilizează acest calculator, este recomandat să vă protejați setările de control parental cu o parolă. Setând parola, veți împiedica alți utilizatori cu drepturi administrative pe sistem să modifice setările de Control parental pe care le-ați configurat pentru un anumit utilizator.

BitDefender vă va solicita în mod implicit să setați o parolă atunci când activați Controlul parental.



Setați protecția prin parolă

Pentru a seta protecția prin parolă, procedați astfel:

1. Introduceți parola în câmpul **Parolă**.
2. Introduceți parola din nou în câmpul **Confirmă parola**.
3. Faceți clic pe **OK** pentru a salva parola și închide fereastra.

Din acest moment, dacă doriți să schimbați setările de control parental, vi se va solicita să introduceți parola. Ceilalți administratori de sistem, dacă există, vor trebui, de asemenea, să furnizeze parola pentru a putea schimba setările de control parental.

Notă
Această parolă nu va proteja alte setări BitDefender.

Dacă nu setați parola și nu doriți să mai apară această fereastră din nou, bifați **Nu solicita parolă la activarea Controlului parental**.

20.1.2. Setarea categorie de vârstă

Filtrul web euristic analizează paginile web și le blochează pe acelea care prezintă trăsături caracteristice unui conținut potențial inadecvat.

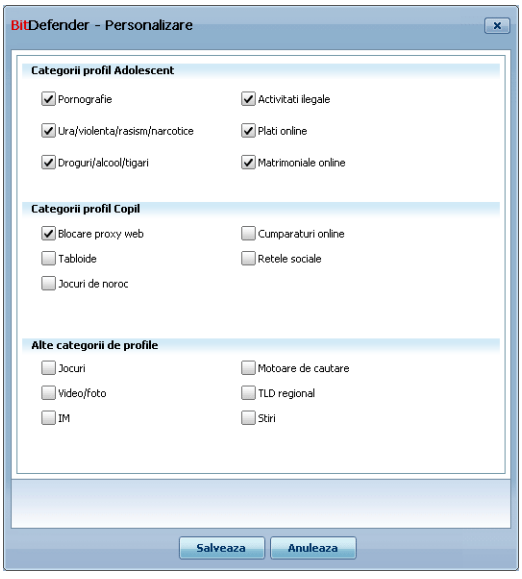
Pentru a filtra accesul web conform unui set de reguli predefinite, bazate pe vârstă, trebuie să setați un anumit nivel de toleranță. Mutați cursorul pentru a seta nivelul de toleranță adecvat pentru utilizatorul selectat.

Există trei niveluri de toleranță:

Nivelul de toleranță	Descriere
Copil	Oferă acces web restricționat, conform setărilor recomandate pentru utilizatori mai mici de 14 ani. Paginile web cu conținut potențial dăunător pentru copii (pornografie, sexualitate, droguri, hacking etc.) sunt blocate.
Adolescent	Oferă acces web restricționat, conform setărilor recomandate pentru utilizatori având vârsta între 14 și 18 ani. Paginile web cu conținut sexual sau pornografic sunt blocate.
Adult	Oferă acces nerestricționat la toate paginile web indiferent de conținutul acestora.

Faceți clic pe **Nivel implicit** pentru a seta cursorul la nivelul implicit.

Dacă doriți să controlați mai bine tipul de conținut la care este expus utilizatorul pe Internet, puteți preciza categoriile de conținut web care vor fi blocate de filtrul web. Pentru a alege tipurile de conținut web care vor fi blocate, faceți clic pe **Categorii personalizate**. Va apărea o nouă fereastră:



Categorii filtru web

Selectați căsuța corespunzătoare categoriei care doriți să fie blocată și utilizatorul nu va mai avea acces la site-urile care fac parte din ea. Pentru ușurarea selecției, categoriile de conținut web sunt afișate pe grupele de vârstă pentru care ar putea fi considerate că sunt adecvate:

- **Categorii profil copil** - include conținut la care pot avea acces copiii subt 14 ani.

Categorie	Descriere
Jocuri	Site-uri web care oferă jocuri bazate pe browsere, forumuri de discuții despre jocuri, posibilitatea de a descărca jocuri, trucuri și instrucțiuni de parcurgere a jocurilor, etc.
Video/Photo	Site-uri web care găzduiesc galerii foto sau video.
IM	Aplicații de mesagerie instant.
Motoare de căutare	Motoare și portaluri de căutare.
TLD regional	Site-uri web care au un nume de domeniu din afara regiunii dvs.
Știri	Ziare online.

- **Categorii profil adolescent** - include conținut care pot fi considerat sigur pentru copii cu vârsta între 14 și 18 de ani.

Categorie	Descriere
Blocare proxy web	Site-uri web folosite pentru a masca adresa URL a unui site solicitat.
Tabloids	Reviste online.
Gambling	Cazinouri online, site-uri pentru pariuri, site-uri care oferă sfaturi legate de pariuri, forumuri despre pariuri, etc.
Online Shopping	Magazine online.
Rețele sociale	Site-uri web ale unor rețele sociale.

- **Categorii profil** - include conținut care nu este adecvat pentru copii și adolescenți.

Categorie	Descriere
Pornography	Site-uri web care găzduiesc conținut pornografic.

Categorie	Descriere
Ură / Violență / Rasism / Narcotice	Site-uri web care găzduiesc conținut cu caracter violent sau rasist, care promovează terorismului sau folosirea narcoticelor.
Droguri / Alcool / Țigări	Site-uri web pe care se vând sau se face publicitate pentru droguri, alcool sau produse din tutun.
Activități ilegale	Site-uri care promovează pirateria sau care găzduiesc conținut piratat.
Online Payment	Formulare pentru plățile online și secțiunile de confirmare a datelor de identificare a cumpărătorilor din magazinele online. Utilizatorul poate naviga prin magazinele online, dar tentativele de achiziționare de produse sunt blocate.
Online Dating	Site-uri web de matrimoniale, cu opțiuni de chat și partajare de fișiere video sau foto.

Faceți clic pe **Aplică** pentru a salva categoriile de conținut web blocate pentru utilizator.

20.2. Monitorizarea activității copiilor

BitDefender vă permite să monitorizați activitățile copiilor dvs pe calculator, chiar și atunci când nu sunteți prezent. Vi se pot trimite alerte prin e-mai de fiecare dată când modulul Control parental blochează o activitate. De asemenea, se poate salva un jurnal cu istoricul site-urilor web vizitate.

Selectați opțiunile pe care doriți să le activați:

- **Trimite-mi un raport de activitate prin e-mail.** O notificare prin e-mail este trimisă de fiecare dată când modulul Control Parental al BitDefender blochează o activitate.
- **Salvează un jurnal de trafic internet.** Înregistrează în jurnal site-urile web vizitate de utilizatorii pentru care este activat Controlul Parental.

20.2.1. Verificarea site-urilor vizitate

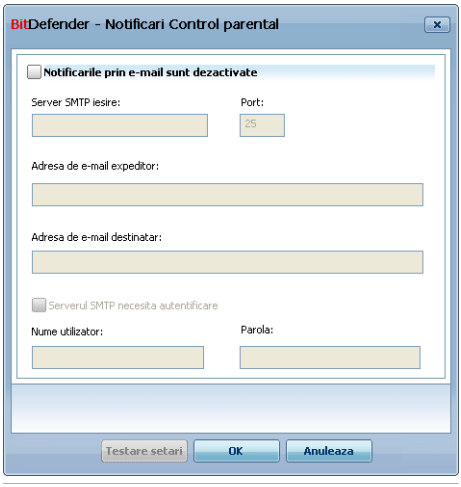
În mod implicit, BitDefender înregistrează în jurnal site-urile web vizitate de copiii dvs.

Pentru a vizualiza fișierele jurnal, faceți clic pe **Vizualizare jurnale** ca să deschideți Istoric&Evenimente și selectați **Jurnal Internet**.

20.2.2. Configurarea notificărilor prin e-mail

Pentru a primi notificări prin e-mail când Controlul parental blochează o activitate, selectați **Trimite-mi un raport de activitate prin e-mail** în fereastra de configurare generală a Controlului parental. Vi se va solicita configurarea setărilor contului dvs de e-mail. Faceți clic pe **Da** pentru a deschide fereastra de configurare.

Notă
Puteți deschide fereastra de configurare, mai târziu, făcând clic pe **Setări notificări**.



Setări de e-mail

Puteți să configurați setările contului dvs de e-mail, după cum urmează:

- **Server SMTP la ieșire** - introduceți adresa serverului de mail folosit pentru trimiterea mesajelor e-mail.
- Dacă serverul utilizează un alt port decât cel implicit, portul 25, introduceți numărul acestuia în câmpul corespunzător.
- **Adresa de e-mail a expeditorului** - introduceți adresa care doriți să apară în câmpul **De la**al e-mail-ului.
- **Adresa de e-mail a destinatarului** - introduceți adresa către care doriți să fie trimise rapoartele prin e-mail.
- Dacă serverul necesită autentificare, selectați căsuța **Serverul meu SMTP necesită autentificare** și introduceți numele de utilizator și parola, în câmpurile corespunzătoare.

Notă
Dacă nu știți ce sunt aceste setări, deschideți-vă clientul de e-mail și verificați setările contului dvs.

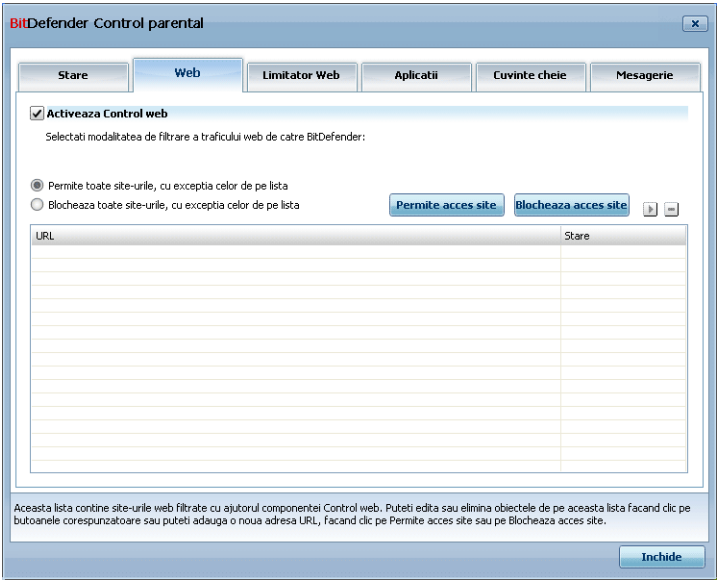
Pentru a valida configurarea, faceți clic pe butonul **Testare setări**. Dacă sunt identificate probleme în timpul validării, BitDefender vă va informa despre aspectele care necesită atenția dvs.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

20.3. Control Web

Controlul Web vă ajută să blocați accesul la paginile web cu conținut inadecvat. O listă cu pagini web propuse spre a fi blocate este oferită de către BitDefender și actualizată permanent, ca parte a procesului obișnuit de actualizare.

Pentru a configura Controlul web pentru un anumit cont de utilizator, faceți clic pe butonul **Modificare** corespunzător acestuia și apoi pe tabul **Web**.



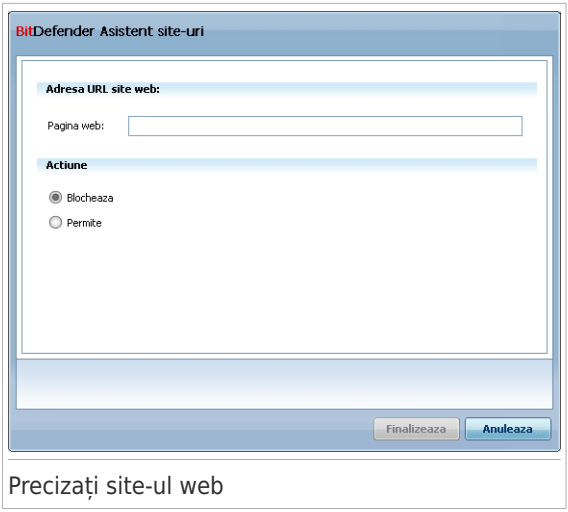
Control Web

Pentru a activa această protecție selectați căsuța corespunzătoare opțiunii **Activează controlul web**.

20.3.1. Crearea regulilor de Control al identității

Pentru a permite sau bloca accesul la un site web, urmați acești pași:

1. Faceți clic pe **Permite site** sau pe **Blochează site**. Va apărea o nouă fereastră:



Precizați site-ul web

2. Introduceți adresa site-ului web în câmpul **Site web**.
3. Selectați acțiunea dorită pentru această regulă - **Permite** sau **Blochează** .
4. Faceți clic pe **Finalizare** pentru a adăuga regula.

20.3.2. Administrarea regulilor de Control al identității

Lista cu Regulile de Control al site-urilor web este prezentată în tabelul din partea de jos a ferestrei. Sunt furnizate adresa site-ului web și starea curentă corespunzătoare fiecărei reguli de Control web.

Pentru a edita o regulă, faceți clic pe butonul **Editează** și faceți modificările necesare în fereastra de configurare. Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge**.

Este necesar să selectați și acțiunea pe care modulul Control parental al BitDefender trebuie s-o aplice site-urilor web pentru care nu există reguli de Control Web:

- **Permite accesul la toate site-urile, cu excepția celor de pe listă**. Selectați această opțiune pentru a permite accesul la toate site-urile web, cu excepția celor pentru care ați setat acțiunea **Blochează**.

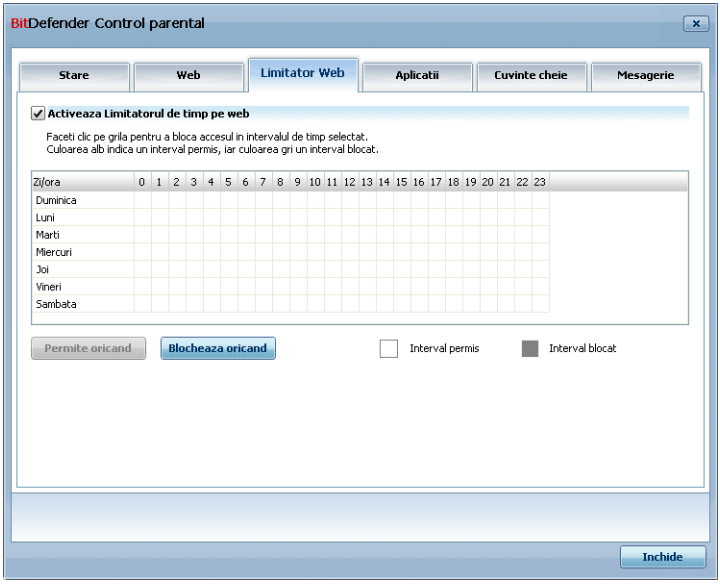
- **Blochează accesul la toate site-urile, cu excepția celor de pe listă**. Selectați această opțiune pentru a bloca accesul la toate site-urile web, cu excepția celor pentru care ați setat acțiunea **Permite**.

20.4. Limitator de timp

Limitatorul de timp vă ajută să permiteți sau să blocați accesul la web pentru utilizatori sau aplicații în timpul anumitor intervale orare.

Notă
BitDefender va realiza actualizări la fiecare oră indiferent de setările **Limitatorului de timp**.

Pentru a configura limitatorul de timp pe web pentru un anumit utilizator, faceți clic pe butonul **Modifică** corespunzător acestuia și apoi pe tabul **Limitator Web**.



Limitator de timp

Pentru a activa această protecție selectați căsuța corespunzătoare opțiunii **Activează limitarea timpului pe web**.

Selectați intervalele de timp în care toate conexiunile la internet vor fi blocate. Puteți face clic pe fiecare celulă în parte, sau puteți selecta perioade mai mari prin clic și tragerea cursorului peste celule.De asemenea, puteți face clic pe **Blochează toate** pentru a selecta toate celulele și, implicit, pentru a bloca complet accesul la

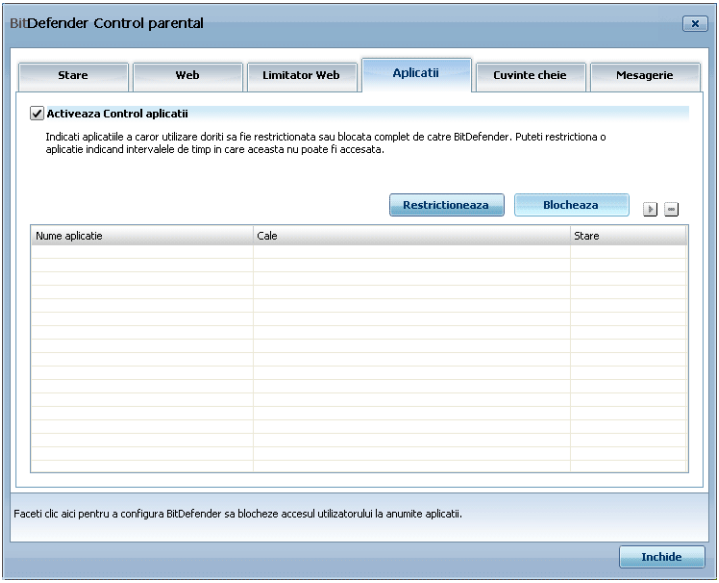
web. Dacă faceți clic pe **Permite toate**, se va permite conectarea la internet în permanență.

Important
Căsuțele colorate în gri reprezintă intervalele de timp când toate conexiunile internet sunt blocate.

20.5. Control aplicații

Controlul aplicațiilor vă ajută să împiedicați orice aplicație să ruleze. Jocurile, softul media și de mesagerie, precum și alte categorii de soft și aplicații malițioase pot fi împiedicate să ruleze. Aplicațiile blocate în acest fel sunt de asemenea protejate de modificări, și nu pot fi copiate sau mutate. Puteți bloca aplicații permanent sau numai în anumite intervale, cum ar fi cele în care copiii dvs trebuie să-și facă temele.

Pentru a configura Controlul aplicațiilor pentru un anumit cont de utilizator, faceți clic pe butonul **Modificare** corespunzător acestuia și apoi pe tabul **Aplicații**.



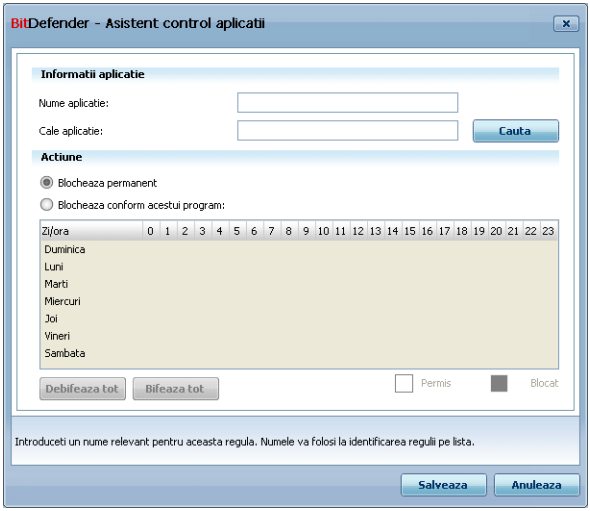
Control aplicații

Pentru a activa această protecție selectați căsuța corespunzătoare opțiunii **Activează controlul aplicațiilor**.

20.5.1. Crearea regulilor de control al aplicațiilor

Pentru a bloca sau a restricționa accesul la o aplicație, urmați pașii de mai jos:

1. Faceți clic pe **Blochează aplicație** sau pe **Restricționează aplicație**. Va apărea o nouă fereastră:



Precizați aplicația

2. Faceți clic pe **Căutare** pentru a localiza aplicația la care doriți să blocați/restricționați accesul.
3. Selectați acțiunea regulii:
   - **Blochează permanent** pentru a bloca complet accesul la aplicație.
   - **Blochează pe baza acestui program** pentru a restricționa accesul în anumite intervale de timp.

   Dacă alegeți să restricționați accesul la aplicație în loc să-l blocați complet, trebuie să și selectați în grilă zilele și intervale de timp în care accesul este blocat. Puteți face clic pe fiecare celulă în parte, sau puteți selecta perioade mai mari prin clic și tragerea cursorului peste celule.De asemenea, puteți face clic pe **Selectare toate** pentru a selecta toate celulele și, implicit, pentru a bloca aplicație complet. Dacă faceți clic pe **Deselectare toate**, aplicația va putea fi accesată oricând.
4. Faceți clic pe **Finalizare** pentru a adăuga regula.

20.5.2. Administrarea regulilor de control al aplicațiilor

Lista cu Regulile de Control al aplicațiilor configurate este prezentată în tabelul din partea de jos a ferestrei. Sunt furnizate numele, calea și starea actuală a fiecărei reguli de Control al aplicațiilor.

Pentru a edita o regulă, faceți clic pe butonul **Editează** și faceți modificările necesare în fereastra de configurare. Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge**.

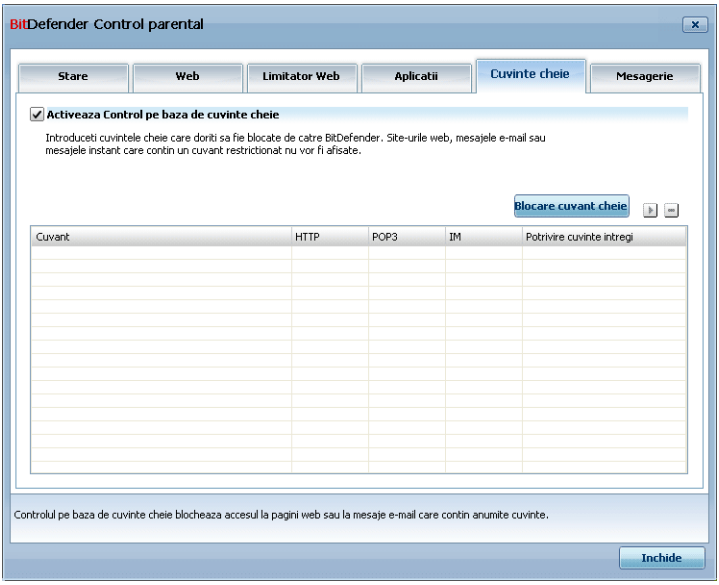
20.6. Control cuvinte cheie

Opțiunea Control cuvinte cheie vă permite să blocați accesul utilizatorilor la mesaje e-mail, pagini web și mesaje instant care conțin anumite cuvinte. Folosind opțiunea Control cuvinte cheie, puteți împiedica vizualizarea de cuvinte sau expresii nepotrivite de către copiii dumneavoastră, atunci când aceștia sunt online.

Notă

Controlul după cuvinte cheie pentru mesageria instant este disponibil numai pentru Yahoo Messenger și Windows Live (MSN) Messenger.

Pentru a configura opțiunea Control cuvinte cheie pentru un anumit cont de utilizator, faceți clic pe butonul **Modificare** corespunzător acestuia și apoi pe tabul **Cuvinte cheie**.



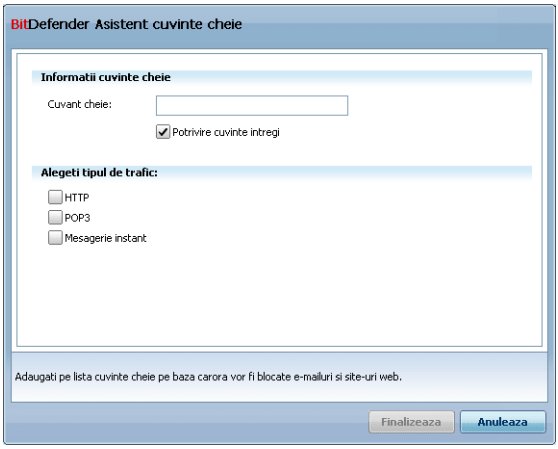
Control cuvinte cheie

Selectați căsuța **Activează Control cuvinte cheie** pentru a folosi această caracteristică de control.

20.6.1. Crearea regulilor de Control cuvinte cheie

Pentru ca blocarea să se facă după un cuvânt sau o sintagmă, urmați acești pași:

1. Faceți clic pe **Blochează cuvânt cheie**. Va apărea o nouă fereastră.



Indicați cuvântul cheie

2. Introduceți cuvântul sau sintagma cheie în câmpul editabil. Dacă doriți să fie detectate numai cuvintele întregi, selectați căsuța **Caută cuvinte întregi**
3. Selectați tipul de trafic pe care BitDefender trebuie să-l scaneze după cuvântul precizat.

Opțiune	Descriere
HTTP	Paginile web care conțin argumentul sunt blocate.
POP3	Mesajele e-mail care conțin argumentul sunt blocate.
Mesagerie instant	Mesajele instant care conțin argumentul sunt blocate.

4. Faceți clic pe **Finalizare** pentru a adăuga regula.

20.6.2. Administrarea regulilor de Control cuvinte cheie

Lista cu Regulile de Control cuvinte cheie este prezentată în tabelul din partea de jos a ferestrei. Sunt furnizate cuvintele cheie și starea actuală a diferitelor tipuri de trafic corespunzătoare fiecărei reguli de Control cuvinte cheie.

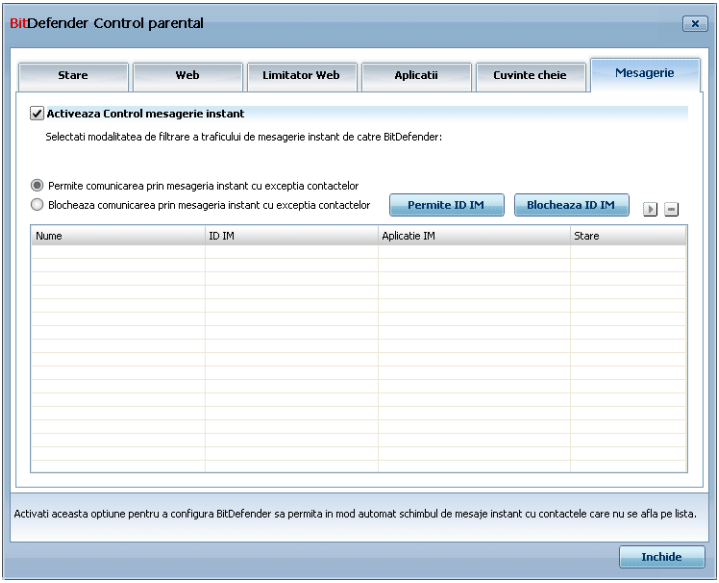
Pentru a edita o regulă, faceți clic pe butonul **Editează** și faceți modificările necesare în fereastra de configurare. Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge**.

20.7. Controlul mesageriei instant

Controlul mesageriei instant vă permite să specificați contactele de mesagerie instant cu care copiii dumneavoastră au voie să converseze.

Notă
Controlul mesageriei instant este disponibil doar pentru Yahoo Messenger și Windows Live (MSN) Messenger.

Pentru a configura Controlul mesageriei instant pentru un anumit cont de utilizator, faceți clic pe butonul **Modificare** corespunzător acestuia și apoi pe tabul **Mesagerie**.



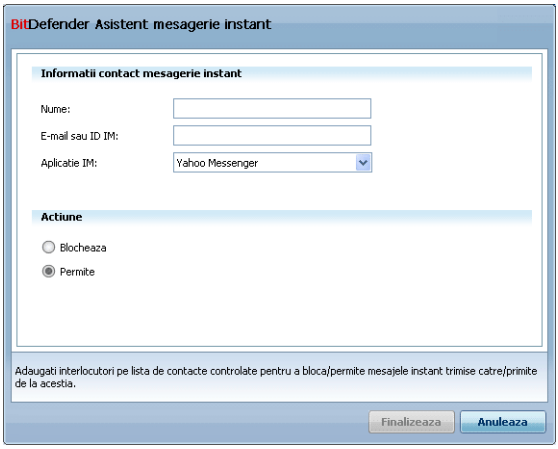
Controlul mesageriei instant

Selectați căsuța **Activează Controlul mesageriei instant** dacă doriți să utilizați această caracteristică de control.

20.7.1. Crearea de reguli de control al mesageriei instant (MI)

Pentru a permite sau bloca schimbul de mesaje instant cu un contact, urmați acești pași:

1. Faceți clic pe **Blochează ID mesagerie instant** sau pe **Permite ID mesagerie instant**. Va apărea o nouă fereastră:



Adăugați contacte IM

2. Introduceți numele interlocutorului în câmpul **Nume**.
3. Introduceți adresa de e-mail sau numele de utilizator folosit de interlocutorul MI în câmpul **E-mail sau ID mesagerie instant**.
4. Selectați programul de mesagerie instant asociat contactului.
5. Selectați acțiunea pentru această regulă - **Blochează** sau **Permite** .
6. Faceți clic pe **Finalizare** pentru a adăuga regula.

20.7.2. Administrarea regulilor de control al mesageriei instant (MI)

Lista cu Regulile de Control al mesageriei instant este prezentată în tabelul din partea de jos a ferestrei. Sunt furnizate numele, ID-ul, aplicația de mesagerie instant și starea actuală corespunzătoare fiecărei reguli de Control al mesageriei instant.

Pentru a edita o regulă, faceți clic pe butonul **Editează** și faceți modificările necesare în fereastra de configurare. Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge**.

De asemenea, trebuie să selectați acțiunea pe care funcția Control parental a BitDefender va trebui s-o aplice contactelor de mesagerie instant pentru care nu s-a creat nicio regulă. Selectați **Blochează** sau **Permite schimbul de mesaje instant cu toate contactele, cu excepția celor de pe listă**.

21. Control date

BitDefender monitorizează zeci de potențiale puncte sensibile ale sistemului dumneavoastră de operare, acolo unde pot acționa aplicațiile spyware, și verifică orice schimbare apărută. Acest modul blochează în mod eficient caii troieni și alte instrumente instalate de hackeri, care încearcă să vă dezvăluie identitatea și să trimită informațiile personale, cum ar fi seria cărții de credit,din computerul dumneavoastră, către hacker.

21.1. Status Control date

Pentru a configura Controlul datelor personale și a vedea informații legate de activitatea acestei opțiuni, faceți clic pe **Control date personale>Stare** în Modul Expert.

Status Control date

Puteți vedea dacă este activat sau nu Controlul datelor. Pentru a schimba starea Controlului datelor, debifați sau selectați căsuța corespunzătoare.

Important
Pentru a preveni furtul de date și a vă proteja identitatea, mențineți activat **Controlul datelor**.

Controlul datelor vă protejează calculatorul prin intermediul următoarelor controale:

- Controlul identității - vă protejează datele confidențiale filtrând traficul web (HTTP), e-mail (SMTP) și de mesagerie instant la ieșirea din calculator potrivit regulilor create de dumneavoastră în secțiunea Identitate.
- Controlul regiștrilor - vă cere permisiunea de fiecare dată când un program încearcă să modifice informațiile din regiștri astfel încât să fie lansat la pornirea Windows.
- Controlul fișierelor cookie - vă cere permisiunea de fiecare dată când un site încearcă să seteze un cookie.
- Controlul scripturilor - vă cere permisiunea de fiecare dată când un domeniu încearcă să ruleze un script sau alt conținut activ.

În partea de jos a acestei secțiuni, puteți vedea **statisticile Controlului datelor**.

21.1.1. Configurarea nivelului de protecție

Puteți alege nivelul de protecție adecvat nevoilor dumneavoastră de securitate. Mutați cursorul pentru a seta nivelul de protecție dorit.

Există trei nivele de protecție:

Nivel de protecție	Descriere
Permisiv	Toate controalele de protecție sunt dezactivate.
Standard	Numai **Control identitate** este activat.
Agresiv	**Control identitate**, **Control registri**, **Control fișiere cookie** și **Control script-uri** sunt activate.

Puteți personaliza nivelul de protecție facând clic pe **Nivel personal**. În fereastra care va apărea, selectați controalele de protecție pe care doriți să le activați și faceți clic pe **OK**.

Faceți clic pe **Nivel implicit** pentru a seta cursorul la nivelul implicit.

21.2. Control identitate

Păstrarea datelor confidențiale în siguranță este o problemă importantă ce ne preocupă pe toți. Furtul de date a ținut pasul cu dezvoltarea comunicațiilor pe Internet și se folosește de noi metode de a păcăli oamenii să cedeze informațiile private.

Fie că este vorba de adresa e-mail sau de numărul cărții de credit, dacă acestea ajung în mâinile unor persoane nepotrivite vă pot aduce daune: puteți să vă treziți că aveți contul de mail plin de spam sau să constatați cu surprindere că aveți contul bancar golit.

Controlul identității vă protejează împotriva furtului de date confidențiale atunci când sunteți online. Pe baza regulilor create de dumneavoastră, Controlul identității scanează traficul web, e-mail sau de mesagerie instant care iese din calculatorul dumneavoastră în căutare de șiruri de caractere specifice (de exemplu, numărul cardului dumneavoastră de credit). Dacă există o concordanță, site-ul web, e-mailul sau mesajul instant respectiv este blocat.

Puteți crea reguli pentru a proteja orice informație pe care o considerați personală sau confidențială, de la numărul dumneavoastră de telefon sau adresa dumneavoastră de e-mail până la informațiile referitoare la contul dumneavoastră bancar. Este oferit suport pentru mai mulți utilizatori, astfel încât utilizatorii care folosesc alte conturi de utilizator Windows să poată configura și folosi propriile reguli de protecție a identității. Dacă aveți un cont Windows de administrator, regulile pe care le creați pot fi configurate să se aplica și atunci când alți utilizatori ai calculatorului sunt conectați la conturile lor Windows.

De ce să folosiți Controlul identității?

- Controlul identității este foarte eficient în blocarea aplicațiilor spyware keylogger. Acest tip de aplicații malițioase înregistrează tot ceea ce tastați și trimite aceste înregistrări prin Internet către o persoană malițioasă (un hacker). Hackerul poate afla din datele furate informații confidențiale, cum ar fi parole și numere de conturi bancare, pe care le va folosi în beneficiul propriu.

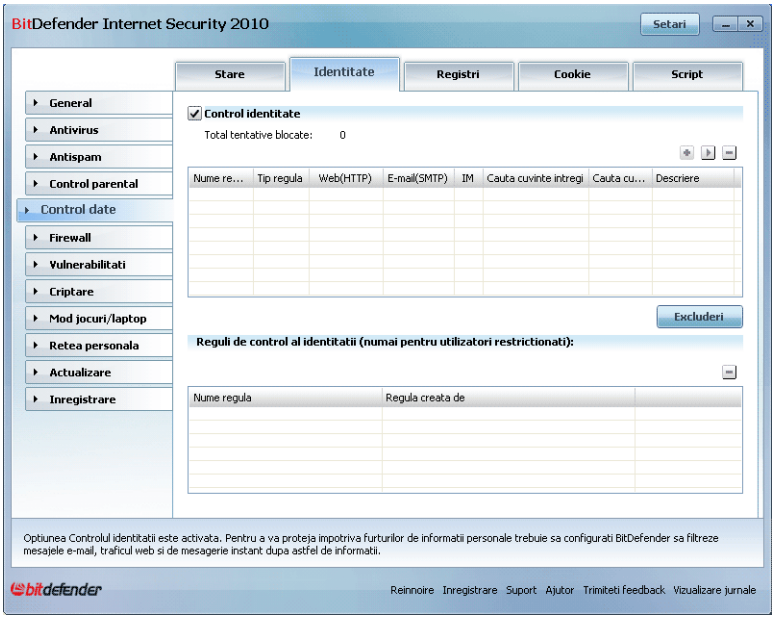
  În eventualitatea în care o astfel de aplicație reușește să evite detecția antivirus, aceasta nu va putea trimite datele furate prin e-mail, web sau mesaje instant, dacă ați creat reguli adecvate de protecție a identității.

- Controlul identității vă poate proteja împotriva tentativelor de phishing (încercări de a fura informații personale). Cele mai frecvente tentative de phishing utilizează un e-mail înșelător pentru a vă convinge să trimiteți informatii personale prin intermediul unei pagini web false.

  De exemplu, puteți primi un e-mail care pare a fi trimis de banca dumneavoastră și care vă solicită să actualizați urgent informațiile de cont bancar. E-mailul conține un link către o pagină web unde trebuie să furnizați informațiile personale. Deși par a fi legitime, e-mailul și pagina web spre care vă trimite linkul înșelător sunt false. Dacă faceți clic pe linkul din e-mail și trimiteți informațiile dumneavoastră personale de pe pagina web falsă, veți dezvălui aceste informații persoanelor răuvoitoare care au organizat înșelătoria.

  Dacă ați creat reguli adecvate de protecție a identității, nu veți putea trimite informații personale (cum ar fi numărul cărții de credit) de pe o pagină web decât dacă ați definit în mod explicit o excepție pentru pagina web respectivă.

Pentru a configura Controlul identității, mergeți la **Control date personale>Identitate** în Modul Expert.



Control identitate

Dacă doriți să utilizați Controlul identității, urmați acești pași:

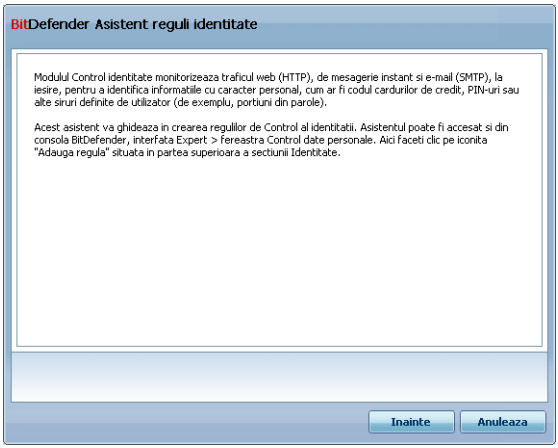
1. Selectați căsuța **Activează Control identitate**.
2. Creați reguli pentru a vă proteja datele confidențiale. Pentru mai multe informații, consultați *„Crearea regulilor de identitate”* (p. 211).
3. Daca este nevoie, stabiliți anumite excepții la regulile pe care le-ați creat. Pentru mai multe informații, consultați *„Definirea excepțiilor”* (p. 214).
4. Dacă sunteți administratorul sistemului, puteți stabili ca regulile de protecție a identității create de alți administratori să nu se aplice în cazul dvs.

   Pentru mai multe informații, consultați *„Regulile stabilite de alți administratori”* (p. 216).

21.2.1. Crearea regulilor de identitate

Pentru a crea o regulă de protecție a identității, faceți clic pe butonul **Adaugă** și urmați pașii programului asistent.

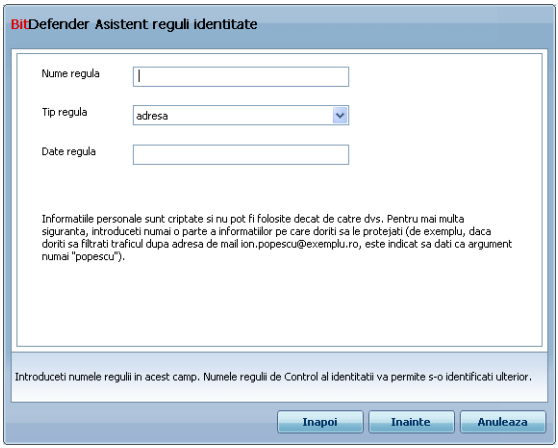
Pasul 1/4 - Fereastra de întâmpinare



Fereastra de întâmpinare

Faceți clic pe **Înainte**.

Pasul 2/4 - Furnizați tipul și argumentul regulei



Furnizați tipul și argumentul regulei

Trebuie setați parametrii următori:

- **Nume regulă** - introduceți numele regulii în acest câmp editabil.
- **Tip regulă** - alegeți tipul regulei (adresă, nume, card de credit, PIN, etc.).
- **Argument regulă** - introduceți datele pe care doriți să le protejați în acest câmp editabil. De exemplu, pentru a vă proteja numărul cardului dumneavoastră de credit, introduceți tot numărul sau doar o parte din el aici.

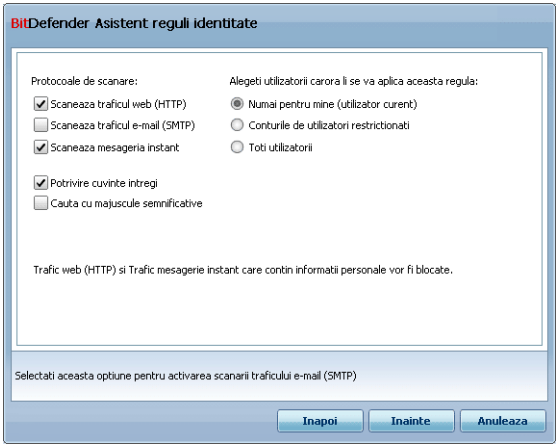
Notă

Dacă introduceți mai puțin de trei caractere, vi se va solicita confirmarea acțiunii. Vă recomandăm să introduceți cel puțin trei caractere pentru a evita blocarea greșită a mesajelor și a paginilor web.

Tot ceea ce introduceți este criptat. Pentru mai multă siguranță, nu introduceți întreaga dată pe care vreți să o protejați ci doar o parte a acesteia.

Faceți clic pe **Înainte**.

Pasul 3/4 - Selectați tipuri de trafic și utilizatori



Selectați tipurile de trafic și utilizatorii

Selectați tipul de trafic care doriți să fie scanat de BitDefender. Următoarele opțiuni sunt disponibile:

- **Scanează web (trafic HTTP)** - scanează traficul HTTP (web) și blochează la ieșire toate datele ce corespund unei reguli.
- **Scanează e-mail (trafic SMTP)** - scanează traficul SMTP (mail) și blochează trimiterea mesajelor e-mail care corespund unei reguli.

- **Scanează MI (mesageria instant)** - scanează traficul de mesagerie instant și blochează trimiterea mesajelor instant care corespund unei reguli.

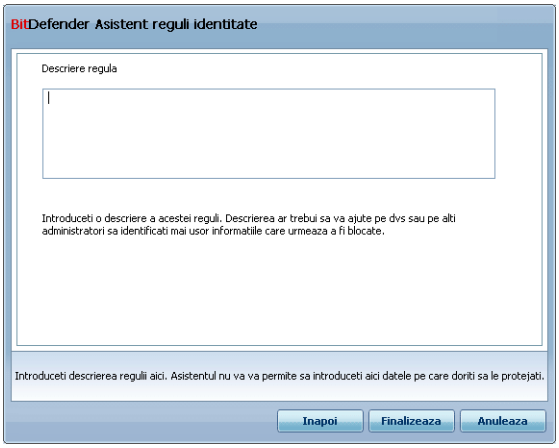
Puteți alege să aplicați regula doar dacă datele protejate apar ca șir independent sau ținând cont de majuscule și minuscule.

Preciyați utilizatorii cărora li se aplica regula.

- **Numai mie (utilizator curent)** - regula se va aplica numai contului dvs de utilizator.
- **Conturi utilizatori cu drepturi limitate** - regula se va aplica numai dvs și tuturor conturilor Windows cu drepturi limitate.
- **Toți utilizatorii** - regula se va aplica tuturor conturilor Windows.

Faceți clic pe **Înainte**.

Pasul 4/4 - Descrieți regula



Descrieți regula

Introduceți o scurtă descriere a regulei în câmpul editabil. Deoarece informația blocată (șirul respectiv de caractere) nu este afișată atunci când este accesată regula, descrierea trebuie să ajute la identificarea acesteia.

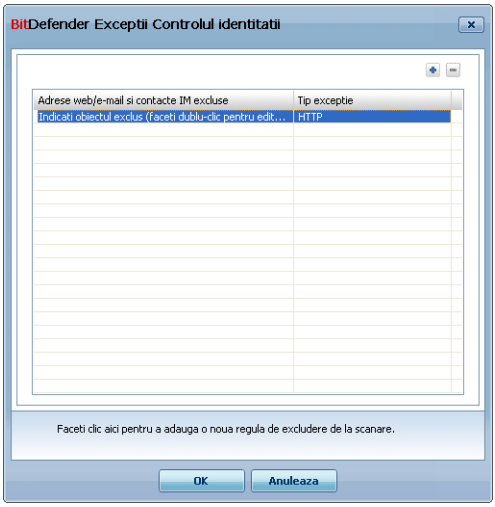
Faceți clic pe **Finalizare**. Regula va apărea în tabel.

21.2.2. Definirea excepțiilor

În unele cazuri, este nevoie să definiți excepții pentru anumite reguli de identitate. Considerați cazul în care creați o regulă de identitate care împiedică trimiterea

numărului cardului dumneavoastră de credit prin HTTP (pe web). De fiecare dată când acesta este trimis pe o pagină web de pe contul dumneavoastră de utilizator, pagina respectivă este blocată. Dacă doriți, de exemplu, să cumpărați o pereche de pantofi prin intermediul unui magazin online (care știți că este securizat), va trebui să specificați o excepție de la regula respectivă.

Pentru a deschide fereastra în care puteți administra excepțiile, faceți clic pe **Excepții**.



Excepții

Pentru a adăuga o excepție, urmați acești pași:

1. Faceți clic pe butonul **Adaugă** pentru a adăuga o nouă înregistrare în tabel.
2. Faceți dublu-clic pe **Specificați obiectul exclus** și introduceți site-ul web, adresa de e-mail sau contactul de mesagerie instant care doriți să fie adăugate ca excepție.
3. Faceți dublu-clic pe **Tip de trafic** și alegeți din meniu opțiunea corespunzătoare tipului de adresă furnizată anterior.
   - Dacă ați specificat o adresă web, selectați **HTTP**.
   - Dacă ați specificat o adresă de e-mail, selectați **E-mail (SMTP)**.
   - Dacă ați specificat un contact IM, selectați **IM**.

Pentru a șterge o excepție de pe listă, selectațiol și faceți clic pe butonul **Șterge**.

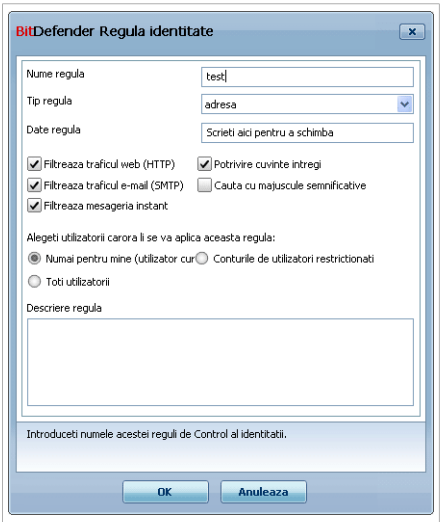
Faceți clic pe **OK** pentru a salva modificările.

21.2.3. Administrarea regulilor

Puteți vedea listate în tabel regulile create până în momentul de față.

Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge**.

Pentru a modifica atributele unei reguli, selectați-o și faceți clic pe butonul **Editează** sau faceți dublu-clic pe ea. Va apărea o nouă fereastră.



Editează regula

Aici puteți modifica numele, descrierea și parametrii regulei (tip, argument și trafic). Faceți clic pe **OK** pentru a salva modificările.

21.2.4. Regulile stabilite de alți administratori

Dacă nu sunteți singurul utilizator cu drepturi de administrare a sistemului, ceilalți administratori pot crea propriile reguli de identitate. Dacă nu doriți ca regulile create de alți utilizatori să vi se aplice când vă conectați, BitDefender vă permite să stabiliți contul dvs de utilizator ca excepție la respectivele reguli.

Puteți vedea o listă de reguli create de alți administratori în tabelul **Reguli de control al identității**. Tabelul conține numele fiecărei reguli și utilizatorului care a creat-o.

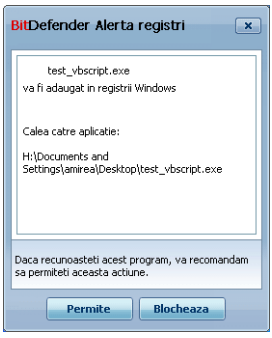
Pentru a vă exclude de la aplicarea unei reguli, selectați regula și faceți clic pe butonul **Șterge**.

21.3. Control regiștri

Una dintre părțile importante ale sistemului de operare Windows sunt **regiștrii**. Aici își păstrează Windows configurația și setările, programele instalate, informații despre utilizator și alte date.

Tot în **regiștri** sunt definite programele care sunt lansate la pornirea Windows. Virușii folosesc des această caracteristică Windows pentru a se lansa automat atunci când utilizatorul își repornește calculatorul.

Controlul Regiștrilor supraveghează regiștrii Windows – în acest fel BitDefender poate detecta troienii. BitDefender vă va alerta de fiecare dată când un program încearcă să modifice informațiile din regiștri astfel încât să fie lansat la pornirea Windows.



Alertă regiștri

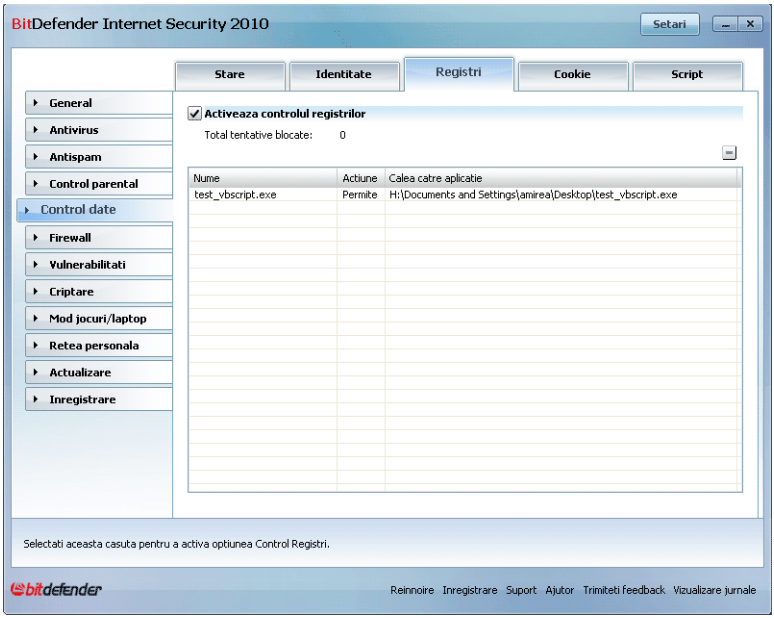
Puteți vedea programul care încearcă să modifice regiștrii Windows.

Dacă nu recunoașteți programul și acesta pare suspect, faceți clic pe **Blochează** pentru a-l împiedica să modifice regiștrii Windows. Altfel, faceți clic pe **Permite** pentru a permite modificarea.

Pe baza răspunsului dumneavoastră, o regulă este creată și listată în tabelul de reguli. Aceeași acțiune este aplicată de fiecare dată când acest program încearcă să modifice o cheie de regiștri.

Notă
BitDefender vă va alerta atunci când instalați programe pentru care este necesară lansarea la pornirea Windows. În cele mai multe cazuri, aceste programe sunt de încredere.

Pentru a configura Controlul identității, mergeți la **Control date personale>Regiștri** în Modul Expert.



Control regiștri

Puteți vedea listate în tabel regulile create până în momentul de față.

Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge**.

21.4. Controlul fișierelor cookie

Fișierele cookie sunt foarte comune pe Internet. Ele sunt fișiere mici salvate pe calculatorul dumneavoastră. Paginile web creează aceste fișiere pentru a vă monitoriza activitatea pe Internet și a salva informații specifice despre dumneavoastră.

În general, fișierele cookie vă fac viața mai ușoară. De exemplu ele ajută site-urile să vă rețină numele și preferințele, pentru a nu trebui să le introduceți la fiecare vizită.

Dar ele pot fi folosite și pentru a vă compromite intimitatea, urmărindu-vă obiceiurile de navigare pe Internet.

Aici vă ajută **Controlul fișierelor cookie**. Când este activat, **Controlul fișierelor cookie** vă va cere permisiunea de fiecare dată când un site încearcă să seteze un cookie:

Alertă cookie

Puteți vedea numele aplicației care încearcă să trimită fișierul cookie.

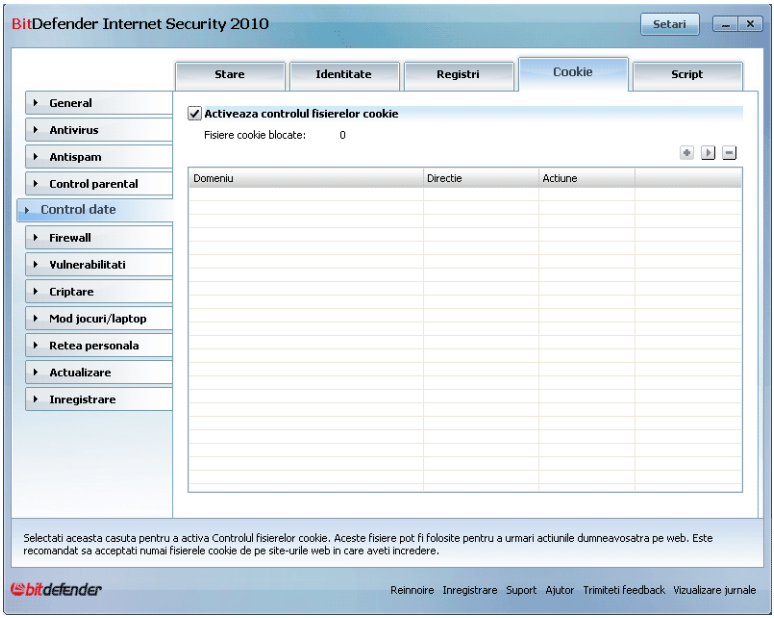
Faceți clic pe **Da** sau pe **Nu** pentru ca o nouă regulă să fie creată, aplicată și menționată în tabelul de reguli.

Aceasta vă va ajuta să alegeți paginile web în care aveți încredere și pe cele în care nu aveți.

Notă

Din cauza numărului mare de fișiere cookie de pe Internet, **Controlul fișierelor cookie** poate fi la început. Inițial, vă va pune foarte multe întrebări despre pagini web care încearcă să seteze cookie-uri pe calculatorul dumneavoastră. După ce adăugați paginile web pe care le folosiți frecvent în lista de reguli, navigarea va deveni la fel de ușoară ca la început.

Pentru a configura Controlul fișierelor cookie, mergeți la **Control date>Cookie** în Modul Expert.



Controlul fișierelor cookie

Puteți vedea listate în tabel regulile create până în momentul de față.

Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge**. Pentru a modifica parametrii regulii, selectați regula și faceți clic sau dublu-clic pe butonul **Editează**. Efectuați modificările dorite în fereastra de configurare.

Pentru a adăuga o regulă manual, faceți clic pe butonul **Adaugă** și configurați parametrii regulii în fereastra de configurare.

21.4.1. Fereastra de configurare

Atunci când editați sau adaugați manual o regulă, va apărea fereastra de configurare.

Selectați adresa, acțiunea și direcția

Puteți seta parametrii:

- **Domeniu** - introduceți adresa domeniului pentru care este creată regula.
- **Acțiune** - selectați acțiunea regulei.

Acțiune	Descriere
Permite	Fișierele cookie ale domeniul respectiv vor fi acceptate.
Interzice	Fișierele cookie ale domeniului respectiv vor fi blocate.

- **Direcție** - selectați direcția traficului.

Tip	Descriere
La ieșire	Regula se aplică numai fișierelor cookie trimise înapoi către siteul de la care au pornit.
La intrare	Regula se aplică numai fișierelor cookie recepționate.
Ambele	Regula se va aplica în ambele direcții.

Notă
Puteți accepta fișiere cookie fără a le returna: setați acțiunea **Interzice** și direcția **La ieșire**.

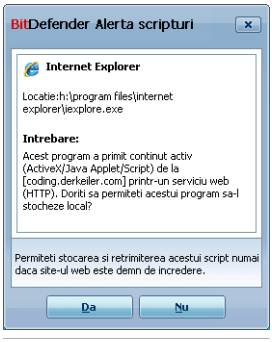
Faceți clic pe **Finalizare**.

21.5. Control scripturi

Scripturile și alte coduri cum ar fi elementele ActiveX și Applet-urile Java, care sunt folosite pentru a crea pagini web, pot fi programate astfel încât să aibă efecte dăunătoare. Elemente de tipul ActiveX, de exemplu, pot avea în întregime acces la datele dumneavoastră și le pot citi sau șterge de pe calculatorul dumneavoastră, pot captura parole și intercepta mesaje cât timp sunteți conectați la Internet. Este recomandat să acceptați conținutul activ doar de la paginile web pe care le cunoașteți foarte bine și care sunt de încredere.

BitDefender vă permite să alegeți să permiteți sau să blocați execuția acestor elemente.

Având **Controlul scripturilor** activat, veți monitoriza adresele web în care aveți încredere și pe cele în care nu aveți. BitDefender vă va cere permisiunea de fiecare dată când un domeniu încearcă să ruleze un script sau alt conținut activ:

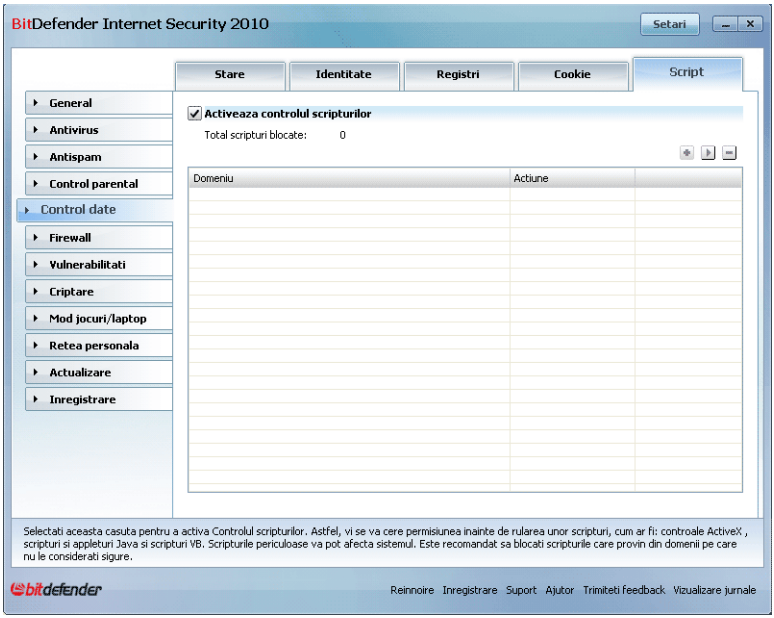


Alertă script

Puteți vedea numele resursei.

Faceți clic pe **Da** sau pe **Nu** pentru ca o nouă regulă să fie creată, aplicată și menționată în tabelul de reguli.

Pentru a configura Controlul script-urilor, mergeți la **Control date personale>Script** în Modul Expert.



Control scripturi

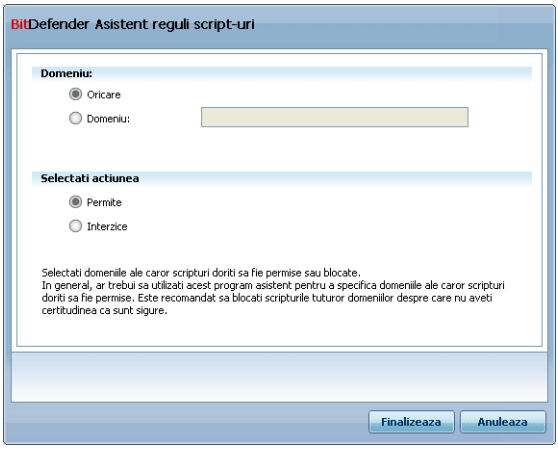
Puteți vedea listate în tabel regulile create până în momentul de față.

Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge**. Pentru a modifica parametrii regulii, selectați regula și faceți clic sau dublu-clic pe butonul **Editează**. Efectuați modificările dorite în fereastra de configurare.

Pentru a crea o regulă manual, faceți clic pe butonul **Adaugă** și configurați parametrii regulii în fereastra de configurare.

21.5.1. Fereastra de configurare

Atunci când editați sau adaugați manual o regulă, va apărea fereastra de configurare.



Selectați adresa și acțiunea

Puteți seta parametrii:

- **Domeniu** - introduceți adresa domeniului pentru care este creată regula.
- **Acțiune** - selectați acțiunea regulei.

Acțiune	Descriere
Permite	Rularea scripturilor este permisă.
Interzice	Rularea scripturilor este interzisă.

Faceți clic pe **Finalizare**.

22. Firewall

Firewallul vă protejează calculatorul de tentative neautorizate de conectare în ambele direcții (la intrare și la iesire). Asemenea unui paznic care stă la ușa dumneavoastră, acest modul va supraveghea conexiunea Internet și va ține o evidență a permisiunilor și a interdicțiilor de acces la Internet.

Notă
În cazul unei conexiuni prin cablu sau DSL este esențial să aveți un firewall.

În Modul ascuns computerul este “ascuns” de aplicațiile malițioase sau de hackeri. Modulul Firewall este capabil să detecteze automat scanări de porturi (pachete trimise către o mașină pentru a găsi puncte de acces, adesea pregătind un atac) și să protejeze calculatorul împotriva acestora.

22.1. Setări

Pentru a configura protecția firewall, mergeți la **Firewall>Setări** în Modul Expert.

Setări Firewall

Puteți vedea dacă firewallul BitDefender este activat sau nu. Pentru a schimba starea firewallului, debifați sau selectați căsuța corespunzătoare.

Important
Pentru a fi protejat de atacuri de pe Internet păstrați modulul**Firewall**activat.

Există două categorii de informații:

- **Sumar configurație rețea.** Puteți vedea numele calculatorului dumneavoastră, adresa IP și gateway-ul acestuia. Dacă aveți mai multe plăci de rețea (sunteți conectat la mai multe rețele), veți vedea adresa IP și gateway-ul configurat pentru fiecare placă de rețea.
- **Statistici.** Puteți vedea statistici variate referitoare la activitatea firewall:
  - numărul de biți trimiși.
  - numărul de biți primiți.
  - numărul de scanări de porturi detectate și blocate de BitDefender. Scanările de porturi sunt folosite în mod frecvent de hackeri pentru a detecta porturi deschise pe calculatorul dumneavoastră cu intenția de a le exploata.
  - numărul de pachete neprelucrate (aruncate).
  - numărul de porturi deschise.
  - numărul de conexiuni la intrare active.
  - numărul de conexiuni la ieșire active.

Pentru a vedea conexiunile active și porturile deschise, mergeți la tabul Activitate.

În partea de jos a secțiunii puteți vizualiza statisticile BitDefender referitoare la traficul la intrare și la ieșire. Graficul arată volumul traficului internet în ultimele două minute.

Notă
Graficul apare chiar dacă modulul **Firewall** este dezactivat.

22.1.1. Setarea acțiunii implicite

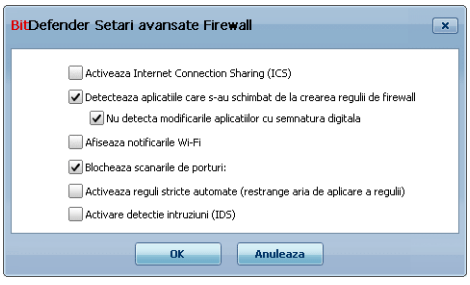
În mod implicit, BitDefender permite automat tuturor programelor din lista de programe cunoscute să acceseze rețeaua și Internetul. Pentru toate celelalte programe, BitDefender vă va solicita prin intermediul unei ferestre de alertă să specificați acțiunea care să fie aplicată. Acțiunea specificată este aplicată de fiecare dată când respectiva aplicație necesită acces la rețea sau Internet.

Puteți muta cursorul pentru a seta acțiunea implicită care să fie luată asupra aplicațiilor care necesită acces la rețea sau Internet. Următoarele acțiuni implicite sunt disponibile:

Acțiune implicită	Descriere
Permite toate	Aplică regulile curente și permite toate tentativele de trafic care nu se potrivesc niciunei reguli existente, fără niciun avertisment. Această politică nu este recomandată; totuși, ea poate fi utilă administratorilor de rețea și pasionaților de jocuri.
Permite cunoscute	Aplică regulile curente și permite toate tentativele de conectare la ieșire ale programelor cunoscute de BitDefender ca fiind legitime (pe lista albă) fără a solicita permisiunea. Pentru restul tentativelor de conectare, BitDefender vă va solicita permisiunea. Programele cunoscute de BitDefender cuprind cele mai utilizate aplicații de pe mapamond. Sunt incluse aici cele mai cunoscute browsere web, playere audio&video, aplicații de chat și de transfer de fișiere, precum și clienți de servere și programe ale sistemului de operare. Pentru a vedea lista albă completă, faceți clic pe **Vizualizare listă albă** .
Raport	Aplică regulile curente și vă consultă în legătură cu tentativele de trafic care nu se potrivesc niciunei reguli existente.
Interzice toate	Aplică regulile curente și blochează toate tentativele de trafic care nu se potrivesc niciunei reguli existente.

22.1.2. Configurarea setărilor avansate de firewall

Puteți face clic pe **Setări avansate** pentru a configura setările avansate de firewall.



Setări avansate firewall

Următoarele opțiuni sunt disponibile:

- **Activează suportul pentru Internet Connection Sharing(ICS)** - activează suportul pentru Internet Connection Sharing(ICS).

  Notă

  Această opțiune nu activează automat ICS pe sistemul dumneavoastră ci doar permite acest tip de conexiune în cazul în care o activați din sistemul de operare.

  Opțiunea Internet Connection Sharing (ICS) a sistemului de operare permite membrilor unei rețele locale să se conecteze la Internet prin intermediul calculatorului dumneavoastră. Acest lucru este util când beneficiați de o conexiune specială la Internet, cum ar fi una wireless, și doriți să poată fi utilizată și de ceilalți membri ai rețelei.

  Împărțirea conexiunii Internet cu membrii rețelelor locale conduce la mărirea consumului de resurse și implică un anumit grad de risc. De asemenea, vă ocupă unele porturi (cele deschise de membrii ce vă utilizează conexiunea Internet).

- **Detectează aplicațiile care s-au modificat de la crearea regulii de firewall** - verifică fiecare aplicație care încearcă să se conecteze la Internet pentru a vedea dacă aceasta a fost modificată de la adăugarea regulii care îi controlează accesul la Internet. Dacă aplicația a fost modificată, va fi afișată o alertă prin care vi se va cere să permiteți sau să blocați accesul aplicației la Internet.

  În general, aplicațiile sunt modificate în urma actualizărilor. Totuși, există riscul ca acestea să fie modificate de aplicații malițioase, cu scopul de a infecta calculatorul dumneavoastră precum și alte calculatoare din rețea.

  Notă

  Vă recomandăm să țineți această opțiune selectată și să permiteți accesul doar acelor aplicații care vă așteptați să fi fost modificate după ce a fost creată regula care le controlează accesul.

  Aplicațiile semnate sunt presupuse a fi sigure și au un grad sporit de securitate. Puteți selecta **Ignoră modificările aplicațiilor cu semnătură digitală** pentru a permite aplicațiilor semnate și modificate să se conecteze la Internet fără ca dvs sa primiți vreo alertă în legătură cu acest eveniment.

- **Afișează notificări wireless** - dacă sunteți conectat la o rețea fără fir (wireless), afișează ferestre informative privind anumite evenimente din rețea (de exemplu, când un calculator nou s-a conectat la rețea).

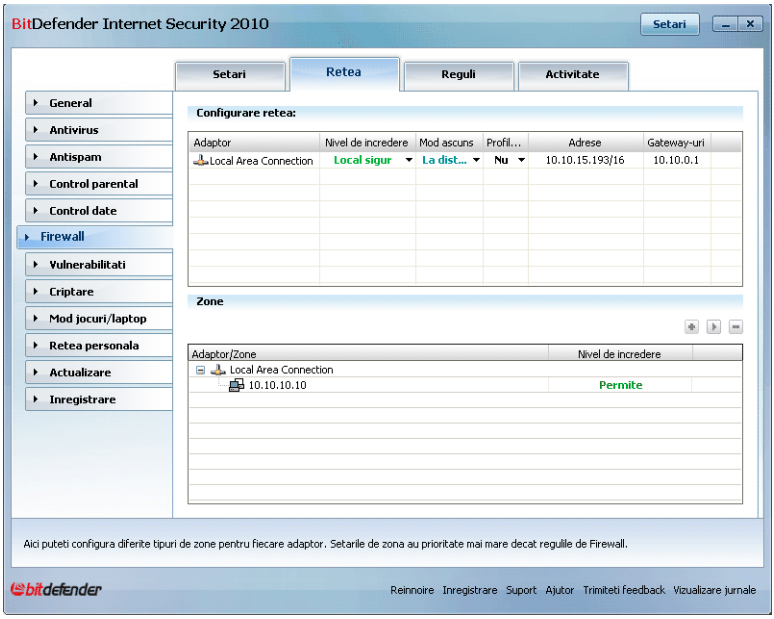
- **Blochează scanările de porturi** - detectează și blochează tentativele de a descoperi care porturi sunt deschise.

  Scanările de porturi sunt folosite în mod frecvent de hackeri pentru a detecta porturi deschise pe calculatorul dumneavoastră. Dacă este detectat un port vulnerabil, aceștia pot pătrunde în calculatorul dumneavoastră.

- **Activează reguli automate stricte** - creează reguli stricte prin intermediul ferestrei de alertă de firewall. Fiind selectată această opțiune, BitDefender vă va solicita să alegeți acțiunea și va crea reguli pentru fiecare proces diferit care deschide aplicația care necesită acces la rețea sau Internet.
- **Activează detecția intruziunilor (IDS)** - activează monitorizarea euristică a aplicațiilor care încearcă să acceseze serviciile de rețea sau Internetul.

22.2. Rețea

Pentru a configura setările firewall, mergeți la **Firewall>Rețea**în Modul Expert.



Rețea

Coloanele din tabelul **Configurație rețea** furnizează informații importante despre rețeaua la care sunteți conectat:

- **Adaptor** - placa de rețea folosită pentru conectarea la rețea sau la Internet.
- **Nivel de încredere** - nivelul de încredere atribuit plăcii de rețea. În funcție de configurația plăcii de rețea, BitDefender va atribui în mod automat un nivel de încredere plăcii de rețea sau vă va solicita informații suplimentare.
- **Modul Ascuns** - dacă puteți fi detectat de alte calculatoare.

- **Profil generic** - dacă sunt aplicate reguli generice pentru această conexiune.
- **Adrese** - adresa IP configurată pentru această placă de rețea.
- **Gateway** - adresa IP folosită de calculatorul dumneavoastră pentru a accesa Internetul.

22.2.1. Modificarea nivelului de încredere

BitDefender atribuie fiecărei plăci (adaptor) de rețea un nivel de încredere. Nivelul de încredere atribuit adaptorului de rețea indică încrederea acordată rețelei.

Pe baza nivelui de încredere, sunt create reguli specifice pentru adaptor privind modul în care sistemul și procesele BitDefender accesează rețeaua și Internetul.

Puteți vedea nivelul de încredere configurat pentru fiecare adaptor în tabelul **Configurare rețea**, sub coloana **Nivel de încredere**. Pentru a modifica nivelul de încredere, faceți clic pe săgeata din coloana **Nivel de încredere** și selectați nivelul dorit.

Nivel de încredere	Descriere
Încredere deplină	Dezactivează firewallul pentru adaptorul respectiv.
Încredere locală	Permite tot traficul dintre calculatorul dumneavoastră și calculatoarele din rețeaua locală.
Sigur	Permite partajarea resurselor cu calculatoare din rețeaua locală. Acest nivel este setat automat pentru rețelele locale (personale sau la birou).
Nesigur	Blochează conectarea calculatoarelor din rețea sau de pe Internet la calculatorul dumneavoastră. Acest nivel este setat automat pentru rețele publice (dacă ați primit o adresă IP de la un furnizor de servicii Internet).
Blocat local	Blochează tot traficul dintre calculatorul dumneavoastră și calculatoarele din rețeaua locală, permițând în același timp accesul la Internet. Acest nivel de încredere este setat automat pentru rețele fără fir (wireless) nesecurizate.
Blocat	Blochează complet traficul de rețea și Internet prin adaptorul respectiv.

22.2.2. Configurarea modului ascuns

În modul ascuns, calculatorul dumneavoastră este ascuns față de aplicații periculoase și de hackeri din rețea sau din Internet. Pentru a configura modul ascuns, faceți clic pe săgeata ▾ din coloana **Ascuns** și selectați opțiunea dorită.

Opțiune	Descriere
Activat	Modul ascuns este activat. Calculatorul dumneavoastră nu poate fi detectat nici din rețeaua locală, nici de pe Internet.
Dezactivat	Modul ascuns este dezactivat. Oricine din rețeaua locală sau de pe Internet poate da ping și detecta calculatorul dumneavoastră.
La distanță	Calculatorul dumneavoastră nu poate fi detectat din Internet. Utilizatorii din rețeaua locală pot da ping și detecta calculatorul dumneavoastră.

22.2.3. Configurarea setărilor generice

Dacă se schimbă adresa IP a unui adaptor de rețea, BitDefender va modifica automat și nivelul de încredere. Dacă doriți să păstrați același nivel de încredere, faceți clic pe săgeata din coloana **Generic** și selectați **Da**.

22.2.4. Zone de rețea

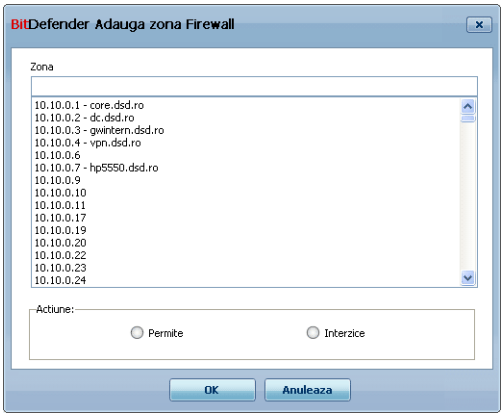
Puteți adăuga calculatoare blocate sau permise pentru un anumit adaptor.

O zonă de încredere este un calculator în care aveți deplină încredere. Tot traficul dintre calculatorul dumneavoastră și un calculator de încredere este permis. Pentru a putea partaja resurse cu calculatoare din rețele fără fir (wireless) nesecurizate, adăugați-le ca fiind calculatoare permise.

O zonă blocată este un calculator care nu doriți să poată comunica sub nicio formă cu calculatorul dumneavoastră.

Tabelul **Zone** afișează zonele curente de rețea pentru fiecare adaptor în parte.

Pentru a adăuga o zonă, faceți clic pe butonul **Adaugă**.



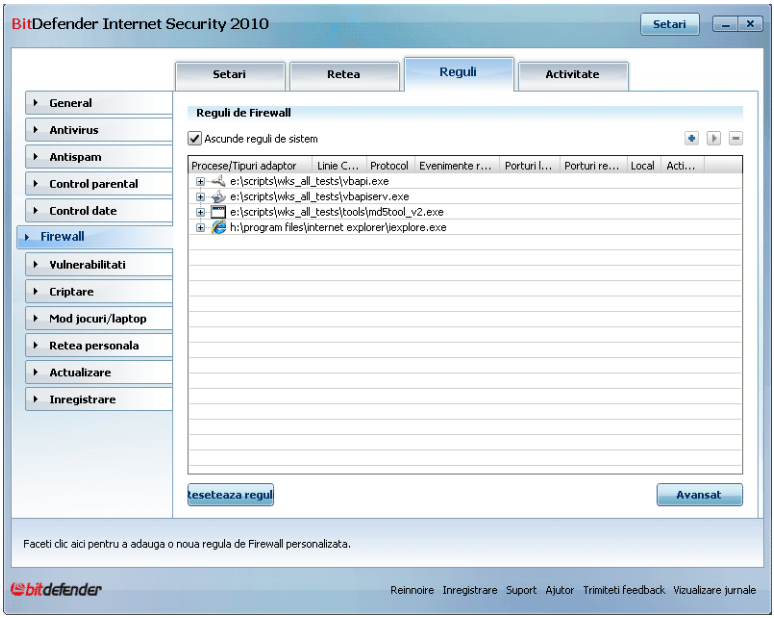
Adăugare zonă

Procedați astfel:

1. Selectați adresa IP a calculatorului pe care doriți să îl adăugați.
2. Selectați acțiunea:
   - **Permite** - pentru a permite tot traficul dintre calculatorul dumneavoastră și calculatorul selectat.
   - **Blochează** - pentru a bloca tot traficul dintre calculatorul dumneavoastră și calculatorul selectat.
3. Faceți clic pe **OK**.

22.3. Reguli

Pentru a administra regulile firewall care controlează accesul aplicațiilor la rețea și Internet, mergeți la **Firewall>Reguli** în Modul Expert.



Reguli firewall

Puteți vedea aplicațiile (procesele) pentru care au fost create reguli firewall. Debifați căsuța **Ascunde regulile de sistem** pentru a vedea și regulile referitoare la procesele de sistem sau la cele ale BitDefender.

Pentru a vedea regulile create pentru o anumită aplicație, faceți clic pe căsuța cu + de lângă aplicația respectivă. Puteți afla informații detaliate despre fiecare regulă din tabel:

- **Proces/Tip adaptor** - procesul și tipul adaptorului de rețea cărora li se aplică regula. Regulile sunt create automat pentru a filtra accesul la rețea sau Internet prin oricare adaptor. Pentru a filtra accesul aplicațiilor la rețea și Internet printr-un anumit adaptor (de exemplu, printr-un adaptor de rețea wireless), puteți crea reguli manual sau puteți edita regulile existente.
- **Linie de comandă** - comanda utilizată în linia de comandă a Windows (**cmd**) pentru a porni procesul.
- **Protocol** - protocolul IP căruia i se aplică regula. Puteți vedea unul dintre următoarele protocoale:

Protocol	Descriere
Oricare	Include toate protocoalele IP.
TCP	TCP, acronimul pentru Transmission Control Protocol, permite stabilirea unei conexiuni si schimbul de date intre 2 sisteme. TCP garantează livrarea de date si primirea pachetelor trimise in aceeași ordine în care au fost expediate.
UDP	UDP, acronimul pentru User Datagram Protocol, este un protocol bazat pe IP proiectat pentru performante ridicate. Jocurile si alte aplicații video folosesc adesea UDP.
Un număr	Reprezintă un anumit protocol IP (altul decât TCP și UDP). Puteți găsi lista completă a numerelor atribuite protocoalelor IP la adresa www.iana.org/assignments/protocol-numbers.

- **Evenimente rețea** - evenimentele de rețea căruia i se aplică regula. Pot fi luate în considerare următoarele evenimente:

Eveniment	Descriere
Conectare	Schimb preliminar de mesaje standard utilizate în cadrul protocoalelor orientate pe conexiune pentru a stabili o conexiune. În cazul protocoalelor orientate pe conexiune, traficul de date dintre două calculatoare apare numai după ce a fost stabilită conexiunea.
Trafic	Schimb de date dintre două calculatoare.
Ascultă	Stare în care o aplicație monitorizează rețeaua așteptând stabilirea unei conexiuni sau recepționarea unor informații de la o aplicație parteneră.

- **Porturi locale** - porturile de pe calculatorul dumneavoastră cărora li se aplică regula.
- **Porturi la distanță** - porturile de pe calculatorul la distanță cărora li se aplică regula.
- **Local** - dacă regula se aplică doar calculatoarelor din rețeaua locală.
- **Acțiune** - dacă aplicației îi este permis accesul la rețea sau Internet în circumstanțele date.

22.3.1. Adăugarea automată a regulilor

Având modulul **Firewall** activat, BitDefender vă va cere permisiunea de fiecare dată când se realizează o conectare la Internet:

Alerta Firewall

Puteți vedea aplicația care încearcă să acceseze internetul, calea către aceasta, destinația, protocolul utilizat și portul prin care aplicația încearcă să se conecteze.

Faceți clic pe **Permite** pentru a permite tot traficul (la intrare și la ieșire) generat de această aplicație de pe calculatorul local către orice destinație, prin protocolul IP respectiv și pe toate porturile. Dacă faceți clic pe **Blochează**, va fi refuzat complet accesul aplicației la Internet prin protocolul IP respectiv.

Pe baza răspunsului dumneavoastră, va fi creată o regulă, care va fi aplicată și listată în tabel. Data viitoare când aplicația va încerca să se conecteze, această regulă va fi aplicată implicit.

Important
Permiteți tentative de conectare la intrare doar de la adrese IP sau domenii în care aveți încredere.

22.3.2. Ștergerea și resetarea regulilor

Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge regulă**. Puteți selecta și șterge mai multe reguli deodată.

Dacă doriți să ștergeți toate regulile create pentru o anumită aplicație, selectați aplicația din listă și faceți clic pe butonul **Șterge regulă**.

Dacă doriți să încărcați setul implicit de reguli stabilit pentru nivelul de încredere selectat, faceți clic pe **Resetare Reguli**.

22.3.3. Crearea și modificarea regulilor

Crearea manuală de noi reguli sau modificarea regulilor existente constă în configurarea parametrilor regulii în fereastra de configurare.

Crearea regulilor. Pentru a crea manual o regulă, urmați acești pași:

1. Faceți clic pe butonul **Adaugă regulă**. Va apărea fereastra de configurare.
2. Configurați parametrii principali și pe cei avansați, după cum este nevoie.
3. Faceți clic pe **OK** pentru a adăuga regula.

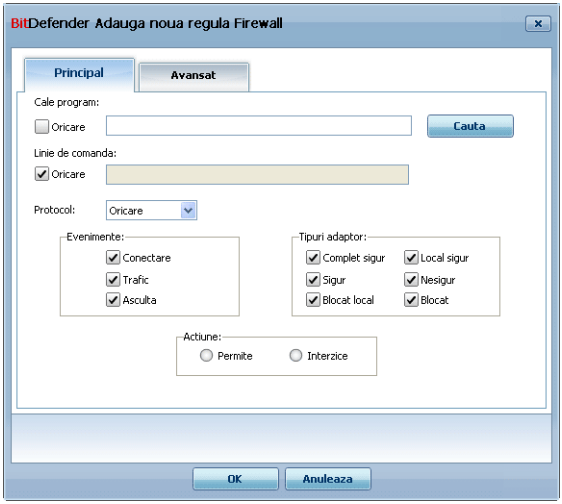
Modificarea regulilor. Pentru a modifica o regulă existentă, urmați acești pași:

1. Faceți clic pe butonul **Editează regula** sau faceți dublu-clic pe regulă. Va apărea fereastra de configurare.

2. Configurați parametrii principali și pe cei avansați, după cum este nevoie.
3. Faceți clic pe **OK** pentru a salva modificările.

Configurarea parametrilor principali

Tabul **Principal** al ferestrei de configurare permite configurarea parametrilor principali ai regulii.



Parametri principali

Puteți configura următorii parametri:

- **Cale program.** Faceți clic pe **Caută** și selectați aplicația căreia i se aplică regula. Dacă doriți care regula să fie aplicată tuturor aplicațiilor, selectați **Oricare**.
- **Linie de comandă.** Dacă doriți ca regula să fie aplicată doar atunci când aplicația selectată este deschisă cu o anumită comandă în linia de comandă Windows, debifați căsuța **Oricare** și introduceți respectiva comandă în câmpul corespunzător.
- **Protocol.** Selectați din meniu protocolul IP căruia i se aplică regula.
  - Dacă doriți ca regula să fie aplicată tuturor protocoalelor, selectați **Oricare**.
  - Dacă doriți ca regula să fie aplicată pentru TCP, selectați **TCP**.
  - Dacă doriți ca regula să fie aplicată pentru UDP, selectați **UDP**.

▶ Dacă doriți ca regula să fie aplicată unui anumit protocol, selectați **Altul**. Va apărea un câmp editabil. Introduceți în câmpul editabil numărul atribuit protocolului care doriți să fie filtrat

Notă

Numerele protocoalelor IP sunt atribuite de către Internet Assigned Numbers Authority (IANA). Puteți găsi lista completă a numerelor atribuite protocoalelor IP la adresa www.iana.org/assignments/protocol-numbers.

- **Evenimente.** În funcție de protocolul selectat, alegeți evenimentele de rețea cărora li se aplică regula. Pot fi luate în considerare următoarele evenimente:

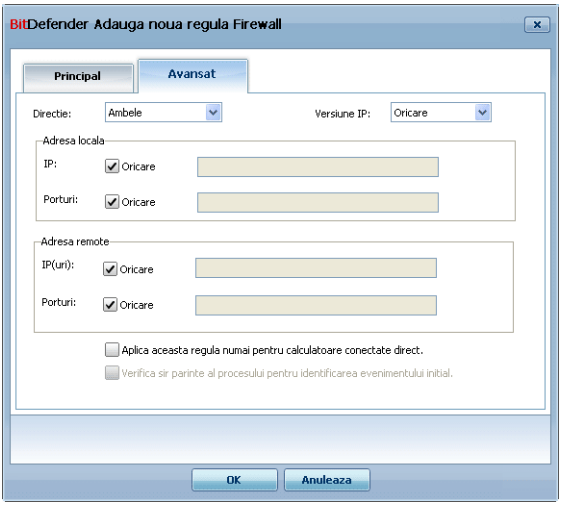
Eveniment	Descriere
Conectare	Schimb preliminar de mesaje standard utilizate în cadrul protocoalelor orientate pe conexiune pentru a stabili o conexiune. În cazul protocoalelor orientate pe conexiune, traficul de date dintre două calculatoare apare numai după ce a fost stabilită conexiunea.
Trafic	Schimb de date dintre două calculatoare.
Ascultă	Stare în care o aplicație monitorizează rețeaua așteptând stabilirea unei conexiuni sau recepționarea unor informații de la o aplicație parteneră.

- **Tipuri de adaptoare.** Selectați tipurile de adaptoare cărora li se aplică regula.
- **Acțiune.** Selectați una dintre acțiunile disponibile:

Acțiune	Descriere
Permite	Aplicației specificate îi va fi permis accesul la rețea / Internet în condițiile specificate.
Interzice	Aplicației specificate îi va fi refuzat accesul la rețea / Internet în condițiile specificate.

Configurarea parametrilor avansați

Tabul **Avansat** al ferestrei de configurare permite configurarea parametrilor avansați ai regulii.



Parametri avansați

Puteți configura următorii parametri avansați:

- **Direcție.** Selectați din meniu direcția traficului căreia i se aplică regula.

Direcție	Descriere
La ieșire	Regula nu se va aplica decât pentru traficul la ieșire.
La intrare	Regula nu se aplica decât pentru traficul la intrare.
Ambele	Regula se va aplica în ambele direcții.

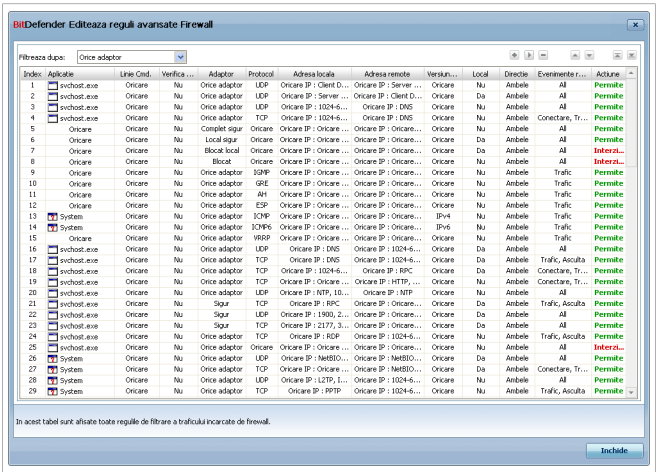
- **Versiune IP.** Selectați din meniu versiunea IP (IPv4, IPv6 sau ambele) căreia i se aplică regula.
- **Adresa locală.** Specificați adresa IP locală și portul local cărora li se aplică regula după cum urmează:
  - Dacă aveți mai multe adaptoare de rețea, puteți debifa căsuța **Oricare** și introduce o anumită adresă IP.
  - Dacă ați selectat TCP sau UDP ca protocol puteți seta un port specific sau o valoare între 0 și 65535. Dacă doriți ca regula să se aplice tuturor porturilor selectați **Oricare**.
- **Adresa la distanță.** Specificați adresa IP și portul la distanță cărora li se aplică regula după cum urmează:

- Pentru a filtra traficul dintre calculatorul dumneavoastră și un anumit calculator, debifați căsuța **Oricare** și introduceți adresa IP a acestuia.
- Dacă ați selectat TCP sau UDP ca protocol puteți seta un port specific sau o valoare între 0 și 65535. Dacă doriți ca regula să se aplice tuturor porturilor selectați **Oricare**.

- **Aplică această regulă doar calculatoarelor direct conectate.** Selectați această opțiune dacă doriți ca regula să fie aplicată doar tentativelor de trafic locale.
- **Verifică procesul părinte al evenimentului original.** Puteți modifica acest parametru doar dacă ați selectat **Reguli automate stricte** (mergeți la tabul Setări și faceți clic pe **Setări avansate**). Reguli stricte înseamnă că BitDefender vă va solicita să alegeți acțiunea când o aplicație necesită acces la rețea sau Internet de fiecare dată când procesul părinte este diferit.

22.3.4. Adminstrarea avansată a regulilor

Dacă doriți să administrați regulile firewall la un nivel avansat, faceți clic pe **Avansat**. Va apărea o nouă fereastră.



Adminstrarea avansată a regulilor

Puteți vedea regulile firewall listate în ordinea în care sunt aplicate. Tabelul furnizează informații complete despre fiecare regulă.

Notă

Atunci când are loc o tentativă de conexiune (la intrare sau la ieșire), BitDefender aplică acțiunea primei reguli care îndeplinește condițiile conexiunii respective. Din acest motiv, ordinea în care sunt verificate aceste reguli este foarte importantă.

Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge regula**.

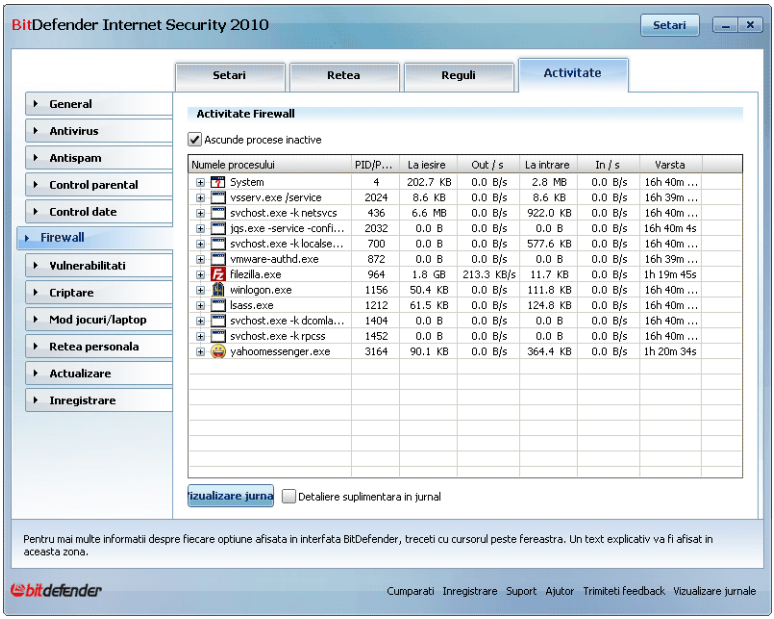
Pentru a modifica o regulă existentă, selectați-o și faceți clic pe butonul **Editează regula** sau faceți dublu-clic pe regulă.

Puteți schimba prioritatea unei reguli. Faceți clic pe butonul **Mută cu un nivel mai sus în listă** pentru a mări prioritatea regulei selectate cu un nivel, sau pe butonul **Mută cu un nivel mai jos în listă** pentru a scădea prioritatea regulei selectate cu un nivel. Pentru a atribui unei reguli prioritatea maximă, faceți clic pe butonul **Mută prima**. Pentru a atribui unei reguli prioritatea minimă, faceți clic pe butonul **Mută ultima**.

Faceți clic pe **Închide** pentru a închide fereastra.

22.4. Control conexiuni

Pentru a monitoriza activitatea curentă în rețea / pe Internet (prin TCP și UDP), sortată pe aplicații, și pentru a deschide jurnalul BitDefender Firewall, mergeți la **Firewall>Activitate** în Modul Expert.



Control conexiuni

Puteți vedea traficul total, sortat după aplicație. Pentru fiecare aplicație, puteți vedea conexiunile și porturile deschise, precum și statistici referitoare la viteza traficului la intrare & ieșire și cantitatea de date trimise / primite.

Dacă doriți să vedeți și procesele inactive, debifați căsuța **Ascunde procesele inactive**.

Sensul iconițelor este după cum urmează:

- Indică o conexiune la ieșire.
- Indică o conexiune la intrare.
- Indică un port deschis pe calculatorul dumneavoastră.

Fereastra prezintă, în timp real, activitatea curentă pe rețea / Internet. Pe măsură ce sunt închise conexiuni și porturi, statisticile corespunzătoare acestora dispar treptat. Același lucru se întâmplă tuturor statisticilor unei aplicații care generează trafic sau are porturi deschise atunci când o închideți.

Pentru o listă completă a evenimentelor referitoare la activitatea modulului Firewall (activare/dezactivare Firewall, blocare trafic, modificare setări) sau generate de activitățile detectate de firewall (scanare de porturi, blocare tentative de conectare sau trafic conform regulilor) accesați fișierul jurnal al BitDefender Firewall făcând

clic pe **Vizualizare jurnal**. Fișierul este localizat în directorul Common Files al utilizatorului Windows curent, la adresa: `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

Dacă doriți ca jurnalul să conțină mai multe informații, selectați opțiunea **Mai multe informații**.

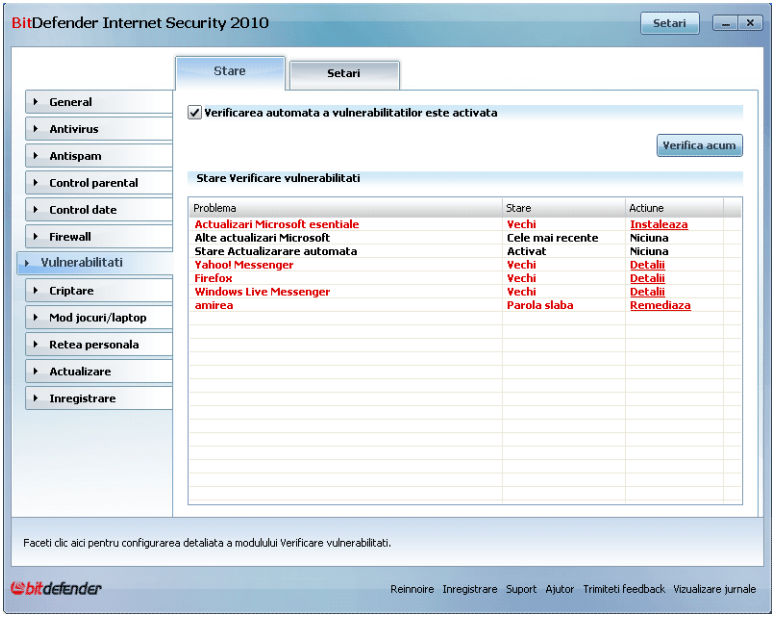
23. Vulnerabilitate

Un pas important în protejarea calculatorului dumneavoastră împotriva persoanelor răuvoitoare și a aplicațiilor malițioase este de a menține actualizat sistemul de operare și aplicațiile pe care le utilizați în mod regulat. De asemenea, pentru a preveni accesul fizic neautorizat la calculatorul dumneavoastră, trebuie configurate parole puternice (parole care nu pot fi ghicite cu ușurință) pentru fiecare cont de utilizator Windows.

BitDefender verifică în mod regulat sistemul dumneavoastră în căutare de vulnerabilități și vă informează despre problemele existente.

23.1. Stare

Pentru a configura verificarea automată a vulnerabilităților sau pentru a verifica vulnerabilitățile sistemului, mergeți la **Vulnerabilitate>Stare** în Modul Expert.



Stare vulnerabilități

În tabel sunt afișate problemele identificate în timpul ultimei verificări a gradului de vulnerabilitate și stadiul acestora. Puteți vedea acțiunea pe care trebuie s-o

aplicați pentru a remedia fiecare vulnerabilitate, dacă este cazul. Dacă se indică **Nicio acțiune**, atunci respectiva problemă nu reprezintă o vulnerabilitate.

Important
Pentru a fi informat automat despre vulnerabilitățile sistemului sau aplicațiilor dumneavoastră, mențineți **Verificarea automată a vulnerabilităților** activată.

23.1.1. Remedierea vulnerabilităților

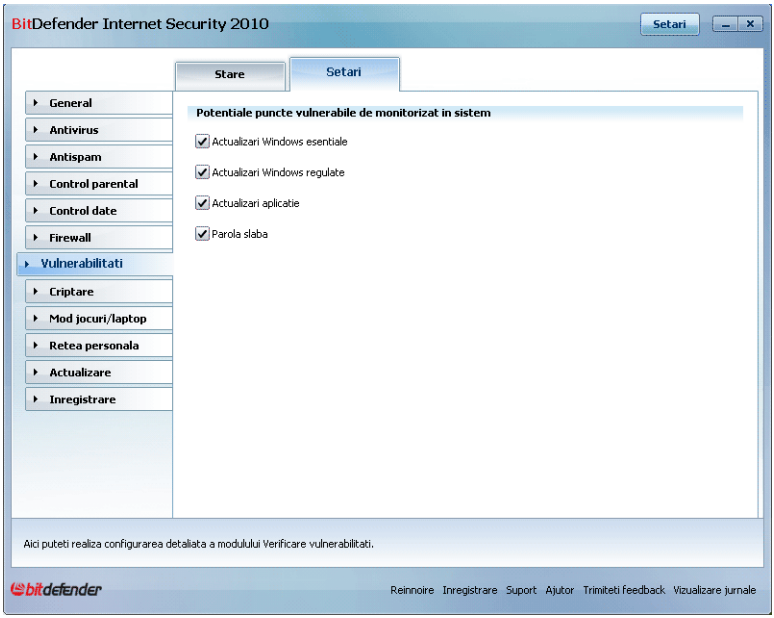
În funcție de problemă, pentru a remedia o anumită vulnerabilitate, procedați după cum urmează:

- Dacă sunt disponibile actualizări Windows, faceți clic pe **Instalează** în coloana **Acțiune** pentru a le instala.
- Dacă există aplicații neactualizate, folosiți linkul **Pagina principală** furnizat, pentru a descărca și instala ultima versiune a respectivei aplicații.
- Dacă un cont de utilizator Windows are o parolă slabă, faceți clic pe **Remediază**, pentru a forța utilizatorul să o modifice la următoarea conectare sau schimbați-o chiar dvs. Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @).

Puteți face clic pe **Verifică acum** și urmați pașii programului asistent pentru a remedia vulnerabilitățile. Pentru mai multe informații, consultați capitolul *„Asistent Verificare vulnerabilități”* (p. 69).

23.2. Setări

Pentru a configura setările verificării automate a vulnerabilităților, mergeți la **Vulnerabilitate>Setări** în Modul Expert.



Setări pentru verificarea automată a vulnerabilităților

Selectați căsuțele corespunzătoare vulnerabilităților care să fie verificate în mod regulat.

- **Actualizări Windows critice**
- **Actualizări Windows obișnuite**
- **Actualizări aplicații**
- **Parole slabe**

Notă

Dacă debifați căsuța corespunzătoare unei anumite vulnerabilități, BitDefender nu vă va mai avertiza despre problemele asociate.

24. Criptare

BitDefender oferă capabilități de criptare pentru a vă proteja documentele confidențiale și conversațiile dumneavoastră prin mesageria instant, prin Yahoo Messenger și MSN Messenger.

24.1. Criptarea mesageriei instant

În mod implicit, BitDefender criptează toate sesiunile dumneavoastră de chat prin mesagerie instant cu condiția ca:

- Partenerul dumneavoastră de chat are instalată o versiune de BitDefender care suportă criptarea mesageriei instant (IM), iar Criptarea IM este activată pentru aplicația de mesagerie instant folosită pentru chat.
- Atât dumneavoastră, cât si partenerul dumneavoastră de chat, să utilizați fie Yahoo Messenger, fie Windows Live (MSN) Messenger.

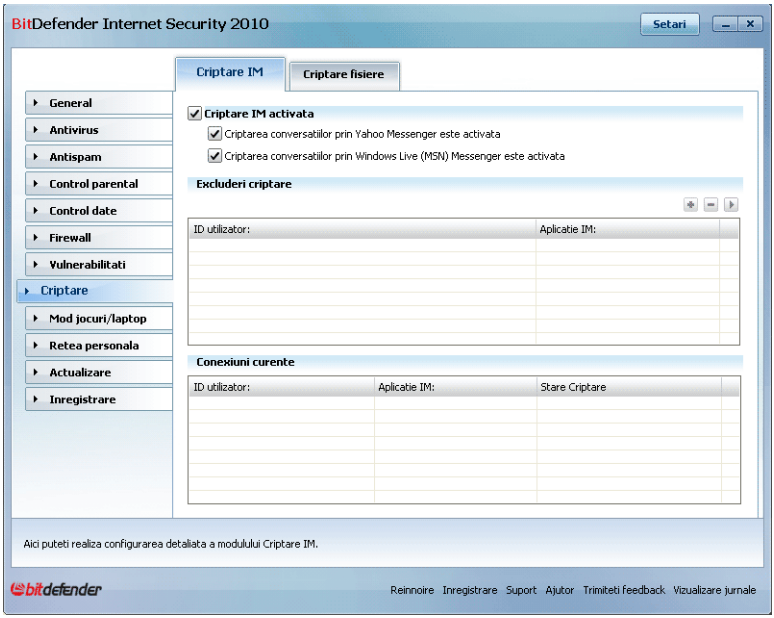
Important

BitDefender nu va cripta o conversație dacă un partener de chat folosește o aplicație web pentru chat, cum ar fi Meebo, sau dacă un partenere folosește Yahoo!, iar celălalt Windows Live (MSN).

Pentru a configura criptarea mesageriei instant, mergeți la **Criptare>Criptare MI** în Modul Expert.

Notă

Puteți configura ușor criptarea mesageriei instant folosind bara de comenzi BitDefender din fereastra de chat. Pentru mai multe informații, va rugam sa accesați *„Integrarea în clienți de mesagerie instant”* (p. 291).



Criptare mesagerie instant

Implicit, criptarea mesageriei instant este activată atât pentru Yahoo Messenger, cât și pentru Windows Live (MSN) Messenger. Puteți alege să dezactivați complet criptarea mesageriei instant sau doar pentru o anumită aplicație de chat.

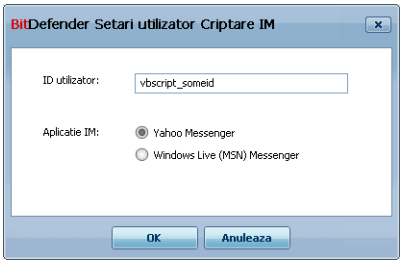
Sunt afișate două tabele:

- **Excluderi criptare** - afișează id-urile de utilizator și programul de mesagerie instant (IM) asociat pentru care criptarea este dezactivată. Pentru a șterge un contact din listă, selectați-l și faceți clic pe butonul **Șterge**.
- **Conexiuni curente** - afișează conexiunile de mesagerie instant curente (ID utilizator și program IM asociat) și dacă aceste conexiuni sunt criptate sau nu. O conexiune poate să nu fie criptată din următoarele motive:
  - Ați dezactivat în mod explicit criptarea pentru contactul respectiv.
  - Contactul dumneavoastră nu are instalată o versiune de BitDefender care oferă criptare IM.

24.1.1. Dezactivarea criptării pentru anumiți utilizatori

Pentru a dezactiva criptarea pentru un anumit utilizator, urmați acești pași:

1. Faceți clic pe butonul **Adaugă** pentru a deschide fereastra de configurare.



Adăugarea contactelor

2. Introduceți în câmpul editabil ID-ul utilizatorului.
3. Selectați aplicația de mesagerie instant asociată contactului.
4. Faceți clic pe **OK**.

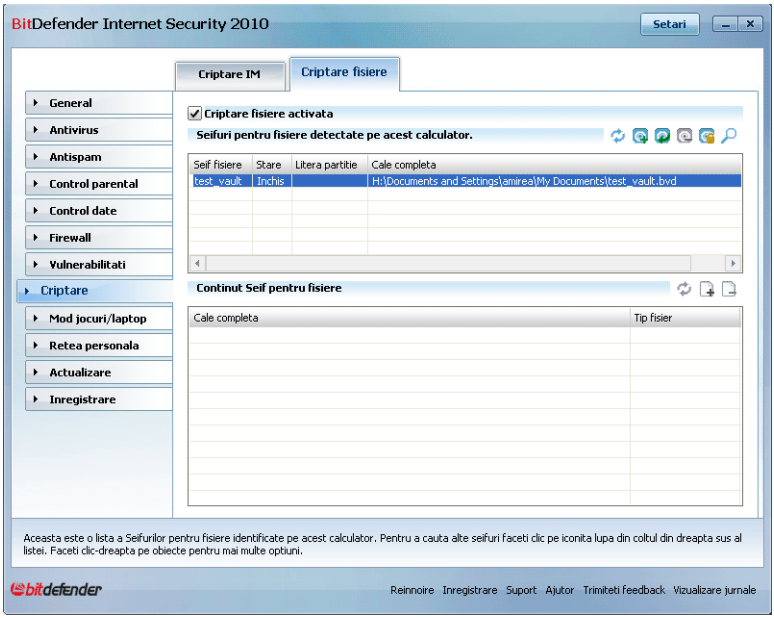
24.2. Criptare fișiere

Opțiunea BitDefender Criptare fișiere vă permite să creați pe calculatorul dumneavoastră partiții logice (seifuri) criptate și protejate prin parolă unde puteți stoca în deplină siguranță documentele dumneavoastră confidențiale. Datele stocate în seifuri pot fi accesate doar de către utilizatorii care cunosc parola.

Parola vă permite să deschideți un seif, să stocați date în acesta și să îl închideți pentru a-i proteja conținutul. Cât timp seifului este deschis, puteți adăuga fișiere noi și puteți accesa sau modifica fișierele existente.

La nivel fizic, seiful este de fapt un fișier criptat de pe hard discul dumneavoastră, având extensia bvd. Deși fișierele fizice reprezentând seifurile pot fi accesate prin intermediul altor sisteme de operare (cum ar fi Linux), informația stocată pe acestea nu poate fi citită deoarece acestea sunt criptate.

Pentru a administra seifurile de fișiere de pe calculatorul dumneavoastră, mergeți la **Criptare>Criptare fișiere** în Modul Expert.



Seif de fișiere

Pentru a dezactiva opțiunea Criptare fișiere, deselectați căsuța **Criptarea fișierelor este activată** și faceți clic pe **Da** pentru confirmare. Dacă dezactivați Seiful de fișiere, toate seifurile de fișiere vor fi închise și nu veți mai putea accesa fișierele pe care acestea le conțin.

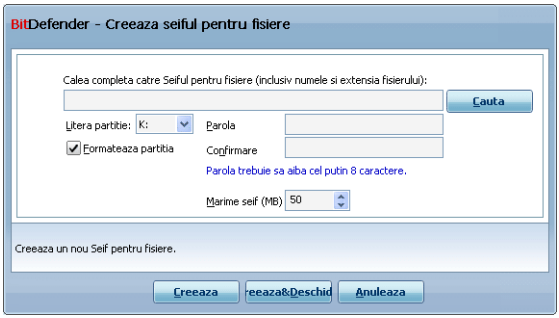
Tabelul din partea de sus afișează seifurile de fișiere de pe calculatorul dumneavoastră. Puteți vedea numele seifului, starea acestuia (deschis / închis), litera partiției corespunzătoare și calea completă către acesta. Tabelul din partea de jos afișează conținutul seifului selectat.

24.2.1. Crearea unui seif

Pentru a crea un seif, utilizați una dintre aceste metode:

- Faceți clic pe **Creează seif**.
- Faceți clic-dreapta în tabelul cu seifuri și selectați **Creează**.
- Faceți clic-dreapta pe desktop sau într-un director de pe calculatorul dumneavoastră, duceți cursorul deasupra opțiunii **Seif BitDefender** și selectați **Creează**.

Va apărea o nouă fereastră.



Creare seif de fișiere

Procedați astfel:

1. Specificați locația și numele seifului de fișiere.
   - Faceți clic pe **Caută**, selectați locația seifului și salvați fișierul seif cu numele dorit.
   - Tastați numele seifului în câmpul corespunzător dacă doriți să fie creat în My Documents. Pentru a deschide My Documents, faceți clic pe meniul Windows Start și apoi pe **My Documents**.
   - Introduceți calea completă pe disc a fișierului seif. De exemplu, `C:\seiful_meu.bvd`.
2. Selectați din meniu o literă pentru partiție. Atunci când deschideți seiful, puteți vedea în My Computer o partiție virtuală denumită cu litera selectată.
3. Introduceți noua parolă a seifului în câmpurile **Parolă nouă** și **Confirmare**. Oricine va încerca să deschidă seiful și să acceseze fișierele acestuia va trebui să furnizeze parola.
4. Selectați **Formatează partiția** pentru a formata partiția virtuală corespunzătoare seifului. Trebuie să formatați partiția virtuală înainte de a putea adăuga fișiere în seif.
5. Dacă doriți să modificați dimensiunea implicită (50 MB) a seifului, introduceți valoarea dorită în câmpul **Dimensiune seif**.
6. Faceți clic pe **Creează** dacă doriți doar să creați seiful în locația selectată. Pentru a crea și a afișa seiful ca partiție virtuală în My Computer, faceți clic pe **Creează&Deschide**.

BitDefender vă va informa imediat despre rezultatul operației. Dacă a avut loc o eroare, utilizați mesajul de eroare pentru a o depana. Faceți clic pe **OK** pentru a închide fereastra.

Notă
Poate fi convenabil să salvați toate seifurile de fișiere în același loc. Astfel, le veți găsi mai ușor.

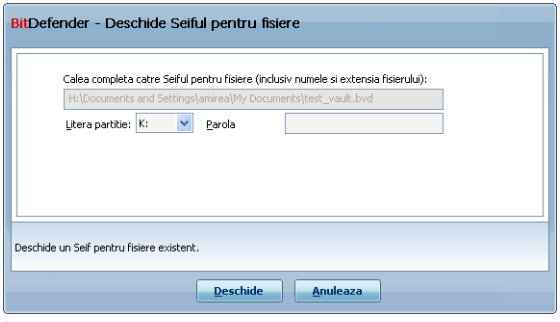
24.2.2. Deschiderea unui seif

Pentru a accesa și a lucra cu fișierele stocate într-un seif, trebuie mai întâi să deschideți seiful. Atunci când deschideți seiful, puteți vedea o partiție virtuală în My Computer. Partiția este denumită cu litera atribuită seifului.

Pentru a deschide seiful, utilizați una dintre aceste metode:

- Selectați seiful din tabel și faceți clic pe **Deschide seif**.
- Faceți clic-dreapta pe seif în tabel și selectați **Deschide**.
- Faceți clic-dreapta pe fișierul seif de pe calculatorul dumneavoastră, duceți cursorul deasupra opțiunii **Seif BitDefender** și selectați **Deschide**.

Va apărea o nouă fereastră.



Deschide seif de fișiere

Procedați astfel:

1. Selectați din meniu o literă pentru partiție.
2. Introduceți parola seifului în câmpul **Parolă**.
3. Faceți clic pe **Deschide**.

BitDefender vă va informa imediat despre rezultatul operației. Dacă a avut loc o eroare, utilizați mesajul de eroare pentru a o depana. Faceți clic pe **OK** pentru a închide fereastra.

24.2.3. Închiderea unui seif

Atunci când ați terminat de lucrat într-un seif de fișiere, trebuie să îl închideți pentru a vă proteja datele. Prin închiderea seifului, partiția virtuală corespunzătoare dispare din My Computer. Ca urmare, este complet blocat accesul la datele stocate în seif.

Pentru a închide un seif, utilizați una dintre aceste metode:

- Selectați seiful din tabel și faceți clic pe **Închide seif**.
- Faceți clic-dreapta pe seif în tabel și selectați **Închide**.
- Faceți clic-dreapta pe partiția virtuală corespunzătoare din My Computer, duceți cursorul deasupra opțiunii **Seif BitDefender** și selectați **Închide**.

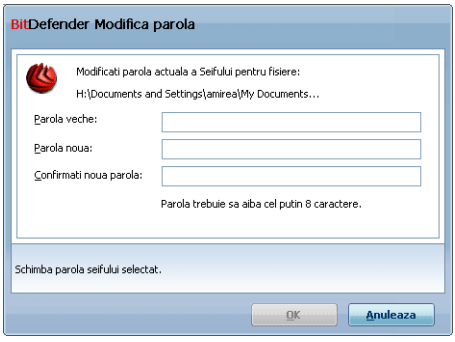
BitDefender vă va informa imediat despre rezultatul operației. Dacă a avut loc o eroare, utilizați mesajul de eroare pentru a o depana. Faceți clic pe **OK** pentru a închide fereastra.

24.2.4. Modificarea parolei seifului

Un seif trebuie să fie închis pentru a-i putea schimba parola. Pentru a modifica parola unui seif, utilizați una dintre aceste metode:

- Selectați seiful din tabel și faceți clic pe **Modifică parola**.
- Faceți clic-dreapta pe seif în tabel și selectați **Modifică parola**.
- Faceți clic-dreapta pe fișierul seif de pe calculatorul dumneavoastră, duceți cursorul deasupra opțiunii **Seif BitDefender** și selectați **Modifică parola**.

Va apărea o nouă fereastră.



Modificare parolă seif

Procedați astfel:

1. Introduceți parola curentă a seifului în câmpul **Parolă curentă**.

2. Introduceți noua parolă a seifului în câmpurile **Parolă nouă** și **Confirmă noua parolă**.

Notă

Parola trebuie să conțină minim 8 caractere. Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @).

3. Faceți clic pe **OK** pentru a salva parola.

BitDefender vă va informa imediat despre rezultatul operației. Dacă a avut loc o eroare, utilizați mesajul de eroare pentru a o depana. Faceți clic pe **OK** pentru a închide fereastra.

24.2.5. Adăugarea fișierelor într-un seif

Pentru a adăuga fișiere într-un seif, urmați acești pași:

1. Selectați seiful în care doriți să adăugați fișiere din tabelul cu seifuri.
2. Dacă seiful este închis, trebuie mai întâi să-l deschideți (faceți clic-dreapta și selectați **Deschide seif**).
3. Faceți clic pe **Adaugă fișier**. Va apărea o nouă fereastră.
4. Selectați fișierele / directoarele pe care doriți să le adăugați în seif.
5. Faceți clic pe **OK** pentru a copia obiectele selectate în seif.

Odată ce seiful este deschis, puteți folosi direct partiția virtuală corespunzătoare seifului. Urmați pașii:

1. Deschideți My Computer (faceți clic pe meniul Windows Start și apoi pe **My Computer**).
2. Intrați în partiția virtuală corespunzătoare seifului. Uitați-vă după litera pe care ați atribuit-o seifului atunci când l-ați deschis.
3. Copiați sau trageți fișiere și directoare direct în această partiție virtuală.

24.2.6. Ștergerea fișierelor dintr-un seif

Pentru a șterge fișiere dintr-un seif, urmați acești pași:

1. Selectați din tabelul cu seifuri seiful care conține fișierul pe care doriți să-l ștergeți.
2. Dacă seiful este închis, trebuie mai întâi să-l deschideți (faceți clic-dreapta și selectați **Deschide seif**).
3. Selectați fișierul pe care doriți să-l ștergeți din tabelul care afișează conținutul seifului.
4. Faceți clic pe **Șterge fișier/directoare**.

Dacă seiful este deschis, puteți șterge direct fișierele de pe partiția logică virtuală corespunzătoare seifului. Urmați pașii:

1. Deschideți My Computer (faceți clic pe meniul Windows Start  și apoi pe **My Computer**).
2. Intrați în partiția virtuală corespunzătoare seifului. Uitați-vă după litera pe care ați atribuit-o seifului atunci când l-ați deschis.
3. Ștergeți fișierele sau directoarele așa cum faceți în mod normal în Windows (de exemplu, faceți clic-dreapta pe un fișier pe care doriți să îl ștergeți și selectați **Delete (Șterge)**).

25. Modul pentru jocuri / laptop

Modul pentru jocuri / laptop vă permite să configurați modurile de funcționare speciale ale BitDefender:

- Modul pentru jocuri modifică temporar setările produsului pentru a minimiza impactul acestora asupra performanței sistemului.
- Modul pentru laptop blochează executarea sarcinilor planificate atunci când laptopul funcționează pe baterie pentru a nu accelera consumarea acesteia.

25.1. Modul pentru jocuri

Modul pentru jocuri modifică temporar setările produsului pentru a minimiza impactul acestora asupra performanței sistemului. Cât timp modul pentru jocuri este activat, se aplică următoarele setări:

- Toate alertele și pop-upurile BitDefender sunt dezactivate.
- Nivelul protecției în timp real BitDefender este setat pe **Permisiv**.
- Firewallul BitDefender este setat pe **Permite tot**. Aceasta înseamnă că toate conexiunile noi (atât la intrare cât și la ieșire) sunt permise în mod automat, indiferent de portul și protocolul utilizat.
- Actualizările nu sunt efectuate în mod implicit.

Notă

Pentru a modifica această setare, mergeți la Actualizare>Setări și debifați căsuța **Nu actualiza dacă este activat modul pentru jocuri**.

- Sarcinile de scanare programate sunt dezactivate în mod implicit.

În mod implicit, BitDefender intră automat în modul pentru jocuri când porniți un joc din lista de jocuri cunoscute a BitDefender sau când o aplicație ocupă întreg ecranul (fullscreen). Puteți intra manual în modul pentru jocuri utilizând combinația de taste implicită `Ctrl+Alt+Shift+G`. Este recomandat să ieșiți din modul pentru jocuri atunci când ați terminat jocul (puteți utiliza aceeași combinația de taste implicită `Ctrl+Alt+Shift+G`).

Notă

Cât timp modul pentru jocuri este activat, puteți vedea litera G pe  iconița BitDefender.

Pentru a configura modul pentru jocuri, mergeți la **Mod jocuri/laptop>Mod jocuri** în modul de vizualizare Expert.

Modul pentru jocuri

În partea de sus a secțiunii, puteți vedea starea modului pentru jocuri. Puteți face clic pe **Intră modul pentru jocuri** sau pe **Ieși din modul pentru jocuri** pentru a schimba starea curentă.

25.1.1. Configurarea modului pentru jocuri automat

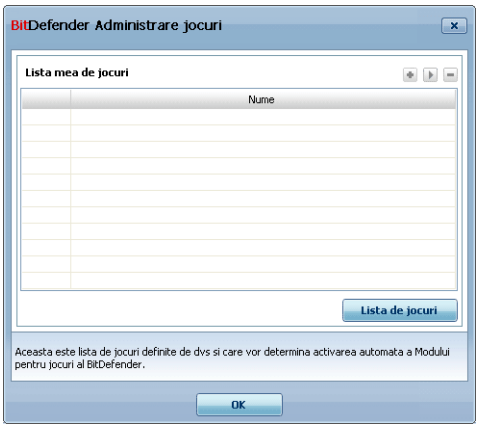
Modul pentru jocuri automat permite BitDefender să intre automat în modul pentru jocuri atunci când este detectat un joc. Puteți configura următoarele opțiuni:

- **Utilizează lista de jocuri furnizată de BitDefender** - pentru a intra automat în modul pentru jocuri când porniți un joc din lista de jocuri cunoscute a BitDefender. Pentru a vedea această listă, faceți clic pe **Administrare jocuri** și apoi pe **Listă jocuri**.
- **Întră în modul pentru jocuri când o aplicație rulează pe ecranul întreg** - pentru a intra automat în Modul pentru jocuri când o aplicație ocupă întregul ecran.
- **Adaugă aplicația pe lista de jocuri?** - pentru a vi se solicita adăugarea unei noi aplicații pe lista de jocuri atunci când aceasta iese din modul ecran întreg. La pornirea unei noi aplicații adăugate pe lista de jocuri, BitDefender va intra automat în modul pentru jocuri.

Notă
Dacă nu doriți ca BitDefender să intre automat în modul pentru jocuri, debifați căsuța **Mod automat pentru jocuri**.

25.1.2. Administrarea listei de jocuri

BitDefender intră automat în modul pentru jocuri atunci când porniți o aplicație din lista de jocuri. Pentru a vedea și administra lista de jocuri, faceți clic pe **Administrare jocuri**. Va apărea o nouă fereastră.



Lista de jocuri

Noi aplicații sunt adăugate în această listă când:

- Porniți un joc de pe lista de jocuri cunoscute a BitDefender. Pentru a vedea această listă, faceți clic pe **Listă jocuri**.
- După ieșirea din full screen, adăugați aplicația în lista de jocuri prin intermediul ferestrei de alertă.

Dacă doriți să dezactivați modul automat pentru jocuri pentru o anumită aplicație din listă, debifați căsuța corespunzătoare acesteia. Puteți dezactiva modul automat pentru jocuri pentru aplicații normale care intră în full screen, cum ar fi browserele web și programele de vizionat filme.

Pentru a administra lista de jocuri, puteți utiliza butoanele plasate în partea de sus a tabelului:

- **Adăugare** - adăugați o nouă aplicație pe lista de jocuri.
- **Eliminare** - eliminați o aplicație de pe lista de jocuri.
- **Editare** - editați un element existent de pe lista de jocuri.

Adăugarea sau editarea jocurilor

Atunci când adăugați sau editați o înregistrare din lista de jocuri, va apărea următoarea fereastră:

Adaugă joc

Faceți clic pe **Caută** pentru a selecta aplicația sau introduceți calea completă către aplicație în câmpul editabil.

Dacă nu doriți ca BitDefender să intre automat în modul pentru jocuri atunci când aplicația selectată este pornită, selectați **Dezactivează**.

Faceți clic pe **OK** pentru a adăuga înregistrarea în lista de jocuri.

25.1.3. Configurarea setărilor modului pentru jocuri

Pentru a configura executarea sarcinilor programate, utilizați aceste opțiuni:

- **Activează acest modul pentru modificarea programelor sarcinilor de scanare antivirus** - pentru a împiedica rularea sarcinilor de scanare programate când Modul pentru jocuri este activat. Puteți selecta una dintre următoarele opțiuni:

Opțiune	Descriere
Sări peste sarcină	Sarcina programată nu este executată deloc.
Amână sarcina	Execută sarcina imediat după ieșirea din modul pentru jocuri.

Pentru a dezactiva automat firewallul BitDefender în modul pentru jocuri, urmați acești pași:

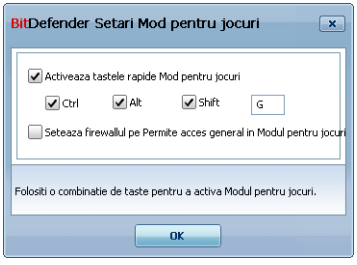
1. Faceți clic pe **Setări avansate**. Va apărea o nouă fereastră.

2. Selectați căsuța **Setează Firewall la Permite tot (Mod pentru jocuri) când este activat Modul pentru jocuri**.
3. Faceți clic pe **OK** pentru a salva modificările.

25.1.4. Schimbarea combinației de taste

Puteți intra manual în modul pentru jocuri utilizând combinația de taste implicită `Ctrl+Alt+Shift+G`. Pentru a schimba combinația de taste, urmați acești pași:

1. Faceți clic pe **Setări avansate**. Va apărea o nouă fereastră.



Setări avansate

2. Sub opțiunea **Utilizează combinația de taste**, setați combinația de taste dorită:
   - Bifați tastele speciale pe care doriți să le folosiți: tasta Control (`Ctrl`), tasta Shift (`Shift`) sau tasta Alternate (`Alt`).
   - În câmpul editabil, tastați litera corespunzătoare tastei normale pe care doriți să o folosiți.

   De exemplu, dacă doriți să folosiți combinația de taste `Ctrl+Alt+D`, trebuie să bifați doar `Ctrl` și `Alt` și să tastați `D`.

   Notă
   Debifarea căsuței corespunzătoare opțiunii **Utilizați combinația de taste** va dezactiva combinația de taste.

3. Faceți clic pe **OK** pentru a salva modificările.

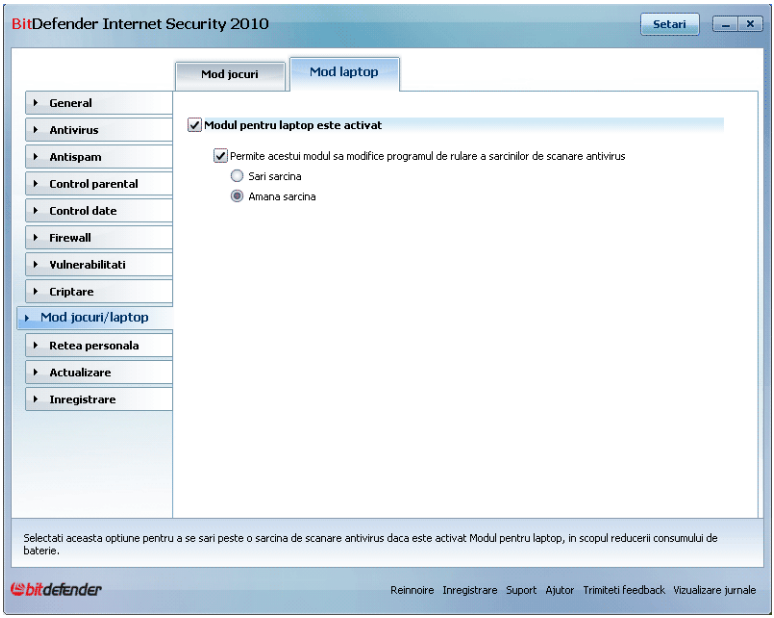
25.2. Modul pentru laptop

Modul pentru laptop este creat special pentru utilizatorii de laptopuri. Scopul acestuia este să minimizeze impactul pe care îl are BitDefender asupra consumului bateriei atunci când aceste dispozitive funcționează pe baterie.

În modul pentru laptop, sarcinile programate nu sunt executate în mod implicit.

BitDefender detectează când laptopul dumneavoastră a trecut pe baterie și intră automat în modul pentru laptop. De asemenea, BitDefender iese automat din modul pentru laptop, atunci când detectează că laptopul nu mai funcționează pe baterie.

Pentru a configura modul pentru laptop, mergeți la **Mod jocuri/laptop>Mod laptop** în modul de vizualizare Expert.



Modul pentru laptop

Puteți vedea dacă modul pentru laptop este activat sau nu. Dacă modul pentru laptop este activat, BitDefender va aplica setările configurate atunci când laptopul funcționează pe baterie.

25.2.1. Configurarea setărilor modului pentru laptop

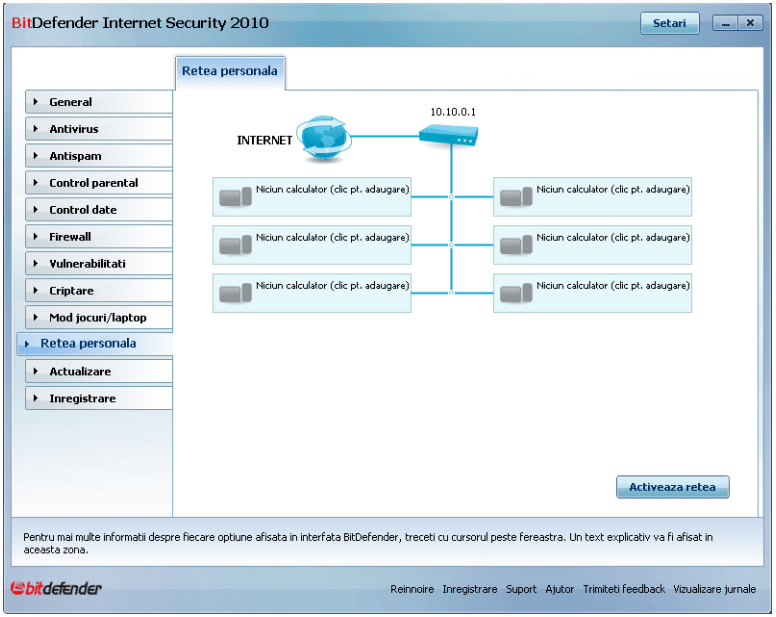
Pentru a configura executarea sarcinilor programate, utilizați aceste opțiuni:

- **Activează acest modul pentru modificarea programelor sarcinilor de scanare antivirus** - pentru a împiedica rularea sarcinilor de scanare programate când Modul pentru laptop este activat. Puteți selecta una dintre următoarele opțiuni:

Opțiune	Descriere
Sări peste sarcină	Sarcina programată nu este executată deloc.
Amână sarcina	Execută sarcina imediat după ieșirea din modul pentru laptop.

26. Rețeaua personală

Modulul Rețea vă permite să administrați produsele BitDefender instalate pe calculatoarele personale de pe un singur calculator.



Hartă rețea

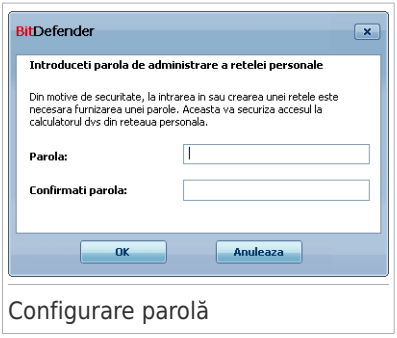
Pentru a putea administra produsele BitDefender instalate pe calculatoarele personale, trebuie să urmați acești pași:

1. Intrați în rețeaua BitDefender personală de pe calculatorul dumneavoastră. Intrarea în rețea constă în configurarea unei parole administrative pentru modulul Rețea.
2. Mergeți la fiecare calculator pe care doriți să-l administrați și intrați în rețea (setați parola).
3. Întoarceți-vă la calculatorul dumneavoastră și adăugați calculatoarele pe care doriți să le administrați.

26.1. Intrarea în rețeaua BitDefender

Pentru a în rețeaua BitDefender personală, urmați acești pași:

1. Faceți clic pe **Activare rețea**. Vi se va cere să configurați parola rețelei personale.



Configurare parolă

2. Introduceți aceeași parolă în ambele câmpuri editabile.
3. Faceți clic pe **OK**.

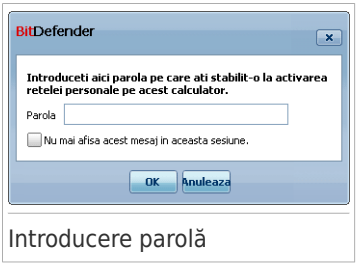
Puteți vedea numele calculatorului apărând pe harta rețelei.

26.2. Adăugarea calculatoarelor la rețeaua BitDefender

Înainte de a putea adăuga un calculator la rețeaua BitDefender personală, trebuie să configurați parola rețelei BitDefender pe calculatorul respectiv.

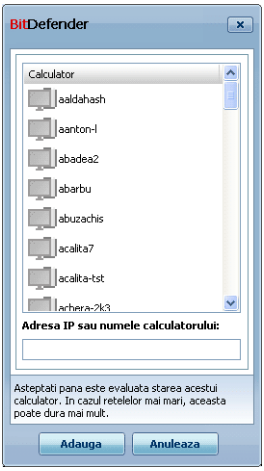
Pentru a adăuga un calculator la rețeaua BitDefender personală, urmați acești pași:

1. Faceți clic pe **Adaugă calculator**. Vi se va cere să furnizați parola locală de administrare a rețelei.



Introducere parolă

2. Introduceți parola de administrare a rețelei și faceți clic pe **OK**. Va apărea o nouă fereastră.



Adaugare calculator

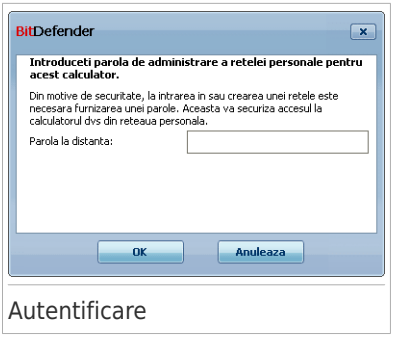
Puteți vedea lista calculatoarelor din rețea. Sensul iconițelor este după cum urmează:

Indică un calculator online fără niciun produs BitDefender instalat.

Indică un calculator online cu BitDefender instalat.

Indică un calculator închis cu BitDefender instalat.

3. Puteți proceda astfel:
   - Selectați din listă numele calculatorului pe care doriți să îl adăugați.
   - Introduceți în câmpul corespunzător adresa IP sau numele calculatorului pe care doriți să îl adăugați.
4. Faceți clic pe **Adaugă**. Vi se va cere să introduceți parola de administrare a rețelei personale configurată pe calculatorul respectiv.



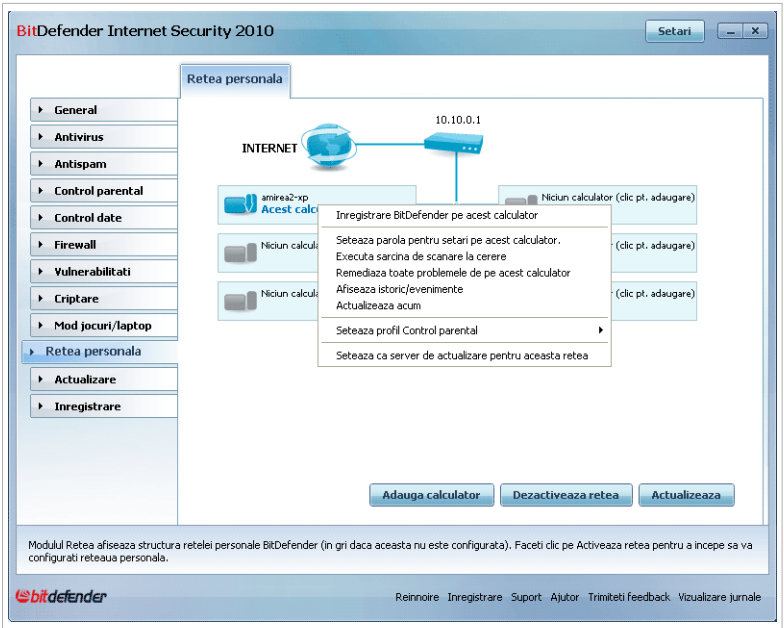
Autentificare

5. Introduceți parola de administrare a rețelei personale configurată pe calculatorul respectiv.
6. Faceți clic pe **OK**. Dacă ați furnizat parola corectă, numele calculatorului selectat va apărea pe harta rețelei.

Notă
Puteți adăuga până la cinci calculatoare pe harta rețelei.

26.3. Administrarea rețelei BitDefender

O dată ce ați creat o rețea BitDefender personală, puteți administra toate produsele BitDefender de pe un singur calculator.



Hartă rețea

Dacă plasați cursorul mouse-ului deasupra unui calculator de pe harta rețelei, puteți vedea informații sumare despre acesta (nume, adresă IP, numărul de probleme care afectează securitatea sistemului, starea înregistrării).

Dacă faceți clic pe numele unui calculator de pe harta rețelei, puteți vedea toate sarcinile administrative pe care le puteți rula de la distanță pe calculatorul respectiv.

- **Scoate calculatorul din rețeaua personală**

  Vă permite să scoateți un calculator din rețea.

- **Înregistrează BitDefender pe acest calculator**

  Vă permite să înregistrați BitDefender pe acest calculator, prin introducerea unei serii de înregistrare.

- **Stabilește o parola pentru setări pe un calculator la distanță**

  Vă permite să creați o parolă pentru a restricționa accesul la setările BitDefender pe acest calculator.

- **Execută o sarcină de scanare la cerere**

Vă permite să executați o scanare la cerere pe calculatorul la distanță. Aveți posibilitatea să efectuați oricare din următoarele sarcini de scanare: Scanare My Documents, scanare de sistem sau scanare profundă de sistem.

- **Remediază toate problemele de pe acest calculator**

  Vă permite să rezolvați problemele care afectează securitatea acestui calculator, urmând pașii programului asistent Remediază probleme.

- **Vizualizare istoric/evenimente**

  Vă permite să accesați modulul **Istoric&Evenimente** al produsului BitDefender instalat pe acest calculator.

- **Update Now**

  Inițiază procesul de Actualizare a produsului BitDefender instalat pe acest calculator.

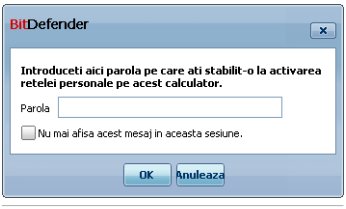
- **Setează profilul de control parental**

  Vă permite să stabiliți categoria de vârstă care va fi folosită de filtrul web al modulului Control Parental pe acest calculator: copil, adolescent sau adult.

- **Stabilește acest calculator ca server de actualizare al acestei rețele**

  Vă permite să setați acest calculator ca server de actualizare pentru toate produsele BitDefender instalate pe calculatoarele din aceasta rețea. Prin folosirea acestei opțiuni, se va reduce traficul pe internet, pentru că numai un calculator din rețea se va conecta la internet pentru a descărca actualizări.

Înainte de a executa o sarcină pe un anumit calculator, vi se va cere să furnizați parola locală de administrare a rețelei.



Introducere parolă

Introduceți parola de administrare a rețelei și faceți clic pe **OK**.

Notă

Dacă doriți să executați mai multe sarcini, puteți bifa **Nu mă mai avertiza în sesiunea curentă**. Selectând această opțiune, nu vi se va mai cere să introduceți această parolă în sesiunea curentă.

27. Actualizare

În fiecare zi sunt descoperite și identificate noi aplicații malițioase. De aceea, este foarte importantă actualizarea BitDefender cu ultimele semnături de aplicații malițioase.

Dacă sunteți conectat la Internet, prin bandă largă sau ADSL, BitDefender se ocupă singur de actualizări. Implicit, BitDefender caută actualizări când deschideți calculatorul și apoi la fiecare **oră**.

Dacă o actualizare este disponibilă, vi se va cere să confirmați actualizarea sau aceasta va fi realizată automat, în funcție de setările de actualizare automată.

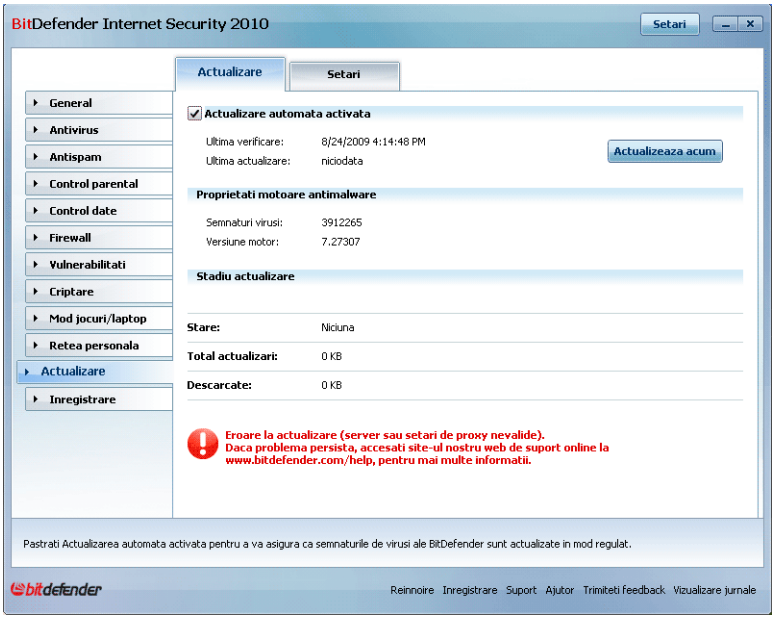
Procesul de actualizare este realizat progresiv, ceea ce inseamna ca fisierele care trebuie actualizate sunt inlocuite unul cate unul. Astfel, procesul de actualizare nu va afecta funcționarea produsului și, în același timp, orice vulnerabilitate va fi exclusă.

Actualizările sunt de mai multe tipuri:

- **Actualizări pentru motoarele Antivirus** - pentru că apar tot timpul noi viruși, fișierele care conțin semnăturile de viruși trebuiesc actualizate pentru a asigura protecție permanentă, la zi, împotriva acestora. Acest tip de actualizare se mai numește **Actualizare definiții viruși**.
- **Actualizări ale motoarelor Antispam** - se vor ad[uga noi reguli filtrelor euristic și URL și noi imagini filtrului de imagine. Astfel, eficiența motorului Antispam va crește. Acest tip de actualizare se mai numește **Actaulizare Antispam**.
- **Actualizări ale motoarelor antispyware** - se vor adăuga noi semnaturi de spyware la baza de date. Acest tip de actualizare se mai numește **Actualizare Antispyware**.
- **Actualizare de produs** - la lansarea unei noi versiuni de produs, noi caracteristici și tehnici de scanare sunt introduse pentru a îmbunătăți performanțele produsului. Acest tip de actualizare se mai numește **Upgrade Produs**.

27.1. Actualizarea Automată

Pentru a vedea informații referitoare la actualizare și pentru a iniția actualizări automate, mergeți la **Actualizare>Actualizare** în Modul Expert.



Actualizarea Automată

Aici puteți vedea când au fost realizate ultima căutare de actualizări și ultima actualizare, precum și informații despre ultima actualizare realizată (dacă a fost reușită sau dacă au apărut erori). De asemenea, sunt afișate informații despre versiunea curentă a motorului de scanare și numărul de semnături.

Dacă deschideți această secțiune în timpul unei actualizări, puteți vedea stadiul acesteia.

Important
Pentru a fi protejat împotriva celor mai noi amenințări, mențineți **Actualizarea automată** activată.

27.1.1. Cererea unei actualizări

Actualizarea automată poate fi realizată oricând făcând clic pe **Actualizează acum**. Acest tip de actualizare este cunoscut și ca **actualizare la cererea utilizatorului**.

Modulul **Actualizare** se va conecta la serverul de actualizare BitDefender și va verifica dacă sunt disponibile noi semnături. Dacă sunt detectate noi semnături, în funcție de opțiunile setate în secțiunea Setări actualizare la cerere, vi se va cere să confirmați actualizarea sau aceasta va fi realizată automat.

Important

Poate fi necesar ca după realizarea unei actualizări să reporniți calculatorul. Este recomandat să faceți acest lucru cât mai repede posibil.

Notă

Dacă vă conectați la Internet prin dial-up, atunci este recomandat să actualizați manual BitDefender în mod regulat.

27.1.2. Dezactivarea actualizării automate

Dacă doriți să dezactivați actualizarea automată, va apărea o fereastră de avertizare. Va trebui să confirmați acțiunea selectând din meniu intervalul de timp pentru care să fie dezactivată actualizarea automată. Puteți dezactiva actualizarea automată pentru 5, 15 sau 30 minute, pentru o oră, permanent sau doar până la repornirea sistemului.

Avertisment

Aceasta este o problemă majoră de securitate. Vă recomandăm să dezactivați actualizarea automată pentru cât mai puțin timp posibil. Dacă nu este actualizat în mod regulat, BitDefender nu va putea să vă protejeze împotriva ultimelor amenințări apărute.

27.2. Setări de Actualizare

Actualizările pot fi realizate din rețeaua locală, de pe Internet, direct sau printr-un server proxy. Implicit, BitDefender va căuta actualizări la fiecare oră, pe Internet, și va instala actualizările disponibile fără a vă mai avertiza.

Pentru a configura setările de actualizare și pentru a administra setările proxy, faceți clic pe **Actualizare>Setări** în Modul Expert.

Setări de Actualizare

Setările de actualizare sunt grupate în patru categorii (**Setări locație de actualizare**, **Setări actualizare automată**, **Setări actualizare la cerere** și **Setări avansate**). Fiecare categorie va fi descrisă separat.

27.2.1. Configurarea locațiilor de actualizare

Pentru a seta locațiile de actualizare, utilizați opțiunile din categoria **Setări locație de actualizare**.

Notă
Configurați aceste setări doar dacă sunteți conectat la o rețea locală care stochează local semnături BitDefender de aplicații malițioase sau dacă vă conectați la Internet printr-un server proxy.

Pentru o actualizare mai sigură și mai rapidă, puteți configura două locații de actualizare: o **Locație de actualizare principală** și o **Locație de actualizare alternativă**. Implicit, acestea sunt setate la fel: `http://upgrade.bitdefender.com`.

Pentru a modifica una dintre locațiile de actualizare, introduceți adresa URL a serverului local în câmpul **URL** corespunzător locației pe care doriți să o modificați.

Notă

Vă recomandăm să setați ca locație principală de actualizare serverul local și să lăsați neschimbată adresa locației de actualizare alternative, ca o măsură de siguranță în caz că serverul local devine indisponibil.

În cazul în care compania utilizează un server proxy pentru conectarea la Internet, selectați **Utilizare proxy** și apoi faceți clic pe **Setări proxy** pentru a configura setările proxy. Pentru mai multe informații, consultați *„Administrarea proxy-urilor”* (p. 273).

27.2.2. Configurarea actualizării automate

Pentru a configura procesul de actualizare realizat automat de BitDefeneder, utilizați opțiunile din categoria **Setări actualizare automată**.

Puteți specifica numărul de ore dintre două căutări consecutive după actualizări în câmpul **Frecvență actualizare**. Intervalul implicit dintre actualizări este de o oră.

Pentru a specifica modul în care să fie realizată actualizarea automată, selectați una dintre următoarele opțiuni:

- **Actualizare discretă** - BitDefender descarcă și realizează actualizarea automat.
- **Anunță înainte de a descărca actualizări** - de fiecare dată când o actualizare este disponibilă, veți fi anunțat înainte de a o descărca.
- **Anunță înainte de a instala actualizări** - de fiecare dată când o actualizare a fost descărcată, veți fi anunțat înainte de a o instala.

27.2.3. Configurarea actualizării manuale

Pentru a specifica cum să fie realizată actualizarea manuală (actualizarea la cererea utilizatorului), selectați una dintre opțiunile din categoria **Setări actualizare manuală**:

- **Actualizare discretă** - actualizarea manuală va fi realizată automat în fundal, fără intervenția utilizatorului.
- **Anunță înainte de a descărca actualizări** - de fiecare dată când o actualizare este disponibilă, veți fi anunțat înainte de a o descărca.

27.2.4. Configurarea setărilor avansate

Pentru ca procesul de actualizare al BitDefender să nu vă afecteze munca, configurați opțiunile din categoria **Setări avansate**:

- **Nu cere restart pentru actualizare** - Dacă o actualizare necesită repornirea sistemului, produsul își va continua funcționarea folosind fișierele vechi până când utilizatorul va reporni calculatorul din proprie inițiativă. Utilizatorului nu i se va cere repornirea calculatorului și astfel actualizarea BitDefender nu va interfera cu activitatea utilizatorului.

- **Nu actualiza dacă o scanare este în progres** - BitDefender nu se va actualiza dacă o scanare este în desfășurare. Astfel, procesul de actualizare BitDefender nu va interfera cu sarcinile de scanare.

  Notă
  Dacă BitDefender este actualizat în timpul unei scanări, procesul de scanare va fi anulat.

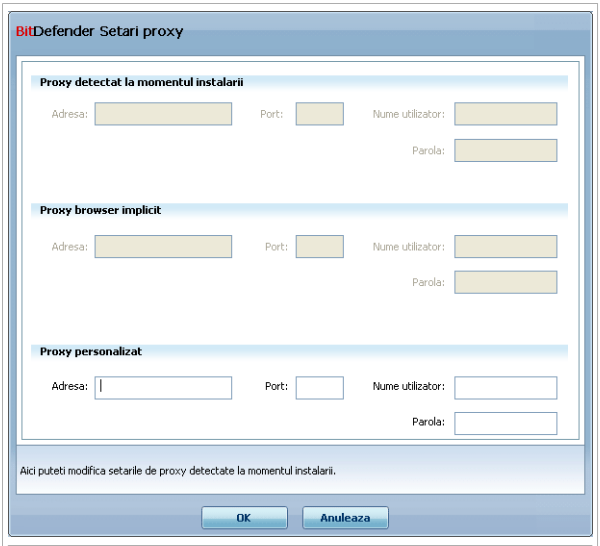
- **Nu actualiza dacă este activat modul pentru jocuri** - BitDefender nu se va actualiza dacă funcționează în modul pentru jocuri. Astfel, puteți minimiza influența produsului asupra performanțelor sistemului în timpul jocului.

27.2.5. Administrarea proxy-urilor

În cazul în care compania utilizează un server proxy pentru conectarea la Internet, trebuie să specificați setările proxy pentru ca BitDefender să se poată actualiza. Altfel, BitDefender va utiliza setările proxy ale administratorului care a instalat produsul sau ale browserului implicit al utilizatorului curent, dacă acestea există.

Notă
Setările proxy pot fi configurate doar de utilizatori cu drepturi administrative pe calculator sau de către utilizatori care cunosc parola produsului.

Pentru a administra setările proxy, faceți clic pe **Setări proxy** . Va apărea o nouă fereastră.



Fereastra de gestionare a setărilor proxy

Există trei seturi de setări proxy:

- **Proxy detectat la instalare** - setări proxy detectate pe contul administratorului în timpul instalării și care pot fi configurate doar dacă sunteți conectat la acel cont. Dacă serverul proxy necesită un nume de utilizator și o parolă pentru autentificare, atunci va trebui să le specificați în câmpurile corespunzătoare.
- **Browser proxy implicit** - setări proxy ale utilizatorului curent, extrase din browserul implicit. Dacă serverul proxy solicită un nume de utilizator și o parolă pentru autentificare, specificați-le în câmpurile corespunzătoare.

Notă

Browserele web suportate sunt Internet Explorer, Mozilla Firefox și Opera. Dacă utilizați un alt browser în mod implicit, BitDefender nu va putea obține setările proxy ale utilizatorului curent.

- **Personalizare proxy** - setări proxy pe care le puteți configura dacă sunteți autentificat ca administrator.

  Următoarele setări trebuie specificate:
  - **Adresă** - introduceți adresa IP a serverului proxy.
  - **Port** - introduceți portul folosit BitDefender pentru a se conecta la serverul proxy.
  - **Utilizator** - introduceți un nume de utilizator recunoscut de proxy.
  - **Parolă** - introduceți o parolă validă pentru numele de utilizator introdus.

Atunci când BitDefender va încerca să se conecteze la Internet, va fi încercat pe rând fiecare set de setări proxy, până când se va reuși conexiunea.

Mai întâi, va fi utilizat setul conținând propriile dumneavoastre setări proxy pentru conectarea la Internet. Dacă acesta nu merge, vor fi încercate în continuare setările proxy detectate la instalare. În sfârșit, dacă nici acestea nu sunt bune, vor fi extrase setările proxy ale utilizatorului curent din browserul implicit și vor fi folosite pentru conectarea la Internet.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Faceți clic pe **Aplică** pentru a salva schimbările sau pe **Implicit** pentru a încărca setările standard.

28. Înregistrare

Pentru a afla informații complete despre produsul dumneavoastră BitDefender și despre stadiul înregistrării, mergeți la **Înregistrare** în Modul Expert.

Înregistrare

Această secțiune afișează:

- **Informații despre produs**: produsul BitDefender și versiunea acestuia.
- **Informații despre înregistrare**: adresa de e-mail utilizată pentru a vă conecta la contul dumneavoastră BitDefender (dacă a fost configurată), seria curentă de înregistrare și câte zile au mai rămas până la expirarea licenței.

28.1. Înregistrarea BitDefender Internet Security 2010

Faceți clic pe **Înregistrare** pentru a deschide fereastra de înregistrare a produsului.

Înregistrare

Puteți vedea starea de înregistrare a produsului dumneavoastră BitDefender, seria curentă de înregistrare și câte zile au mai rămas până la expirarea licenței.

Pentru a înregistra BitDefender Internet Security 2010:

1. Introduceți seria de înregistrare în câmpul editabil.

   Notă
   Puteți găsi seria dumneavoastră de înregistrare:
   - pe eticheta de pe CD.
   - pe certificatul de înregistrare al produsului.
   - în e-mailul de achiziționare online.

   Dacă nu aveți o serie de înregistrare BitDefender, faceți clic pe linkul furnizat pentru a merge la magazinul online BitDefender și a cumpăra una.

2. Faceți clic pe **Înregistrare**.
3. Faceți clic pe **Finalizare**.

28.2. Crearea unui cont BitDefender

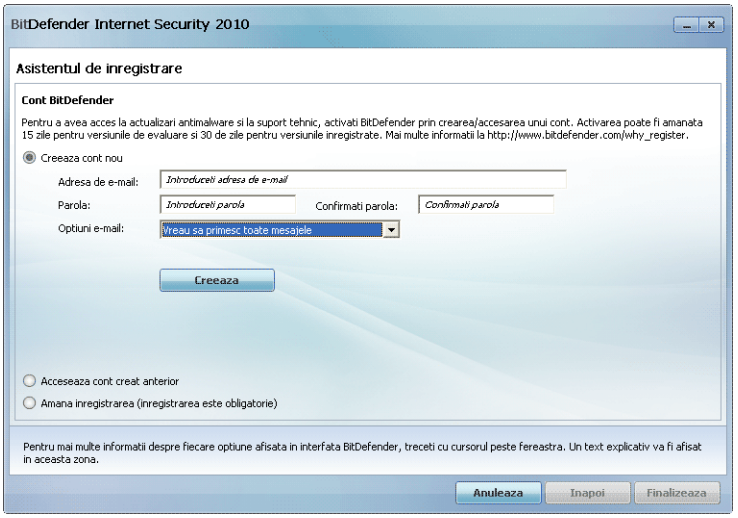
În cadrul procesului de înregistrare, ESTE NECESAR să vă creați un cont BitDefender. Contul BitDefender vă oferă acces la actualizări BitDefender, suport tehnic gratuit, oferte speciale și promoții. Daca v-ați pierdut seria de înregistrare BitDefender,

puteți accesa contul dumneavoastră la http://myaccount.bitdefender.com pentru a o recupera.

Important

Este necesar să vă creați un cont în termen de 15 zile de la instalarea BitDefender (dacă înregistrați produsul cu o serie de înregistrare, termenul limită se extinde la 30 de zile). În caz contrar, BitDefender nu se va mai actualiza.

Dacă nu ați creat încă un cont BitDefender, faceți clic pe **Activează cont** pentru a deschide fereastra de înregistrare a contului.



Creare cont

Dacă nu doriți să creați un cont BitDefender în acest moment, selectați **Amână înregistrarea** si faceți clic pe **Finalizează**. Altfel, continuați în funcție de situația dumneavoastră actuală:

- „Nu am un cont BitDefender” (p. 277)
- „Deja am un cont BitDefender” (p. 278)

Nu am un cont BitDefender

Pentru a crea un cont BitDefender, urmați acești pași:

1. Selectați **Creează cont nou**.

2. Introduceți informațiile solicitate în câmpurile corespunzătoare. Informațiile furnizate aici vor rămâne confidențiale.
   - **Adresă de e-mail** - introduceți adresa dvs. de e-mail.
   - **Parolă** - introduceți o parolă pentru contul dumneavoastră BitDefender. Parola trebuie să conțină între 6 și 16 caractere.
   - **Confirmați parola** - introduceți parola din nou.

   Notă
   După activarea contului, puteți folosi adresa de e-mail și parola furnizate pentru a-l accesa, la adresa http://myaccount.bitdefender.com.

3. Opțional, BitDefender vă poate informa despre oferte speciale și promoții folosind adresa de e-mail a contului dumneavoastră. Selectați una dintre opțiunile disponibile din meniu:
   - **Vreau sa primesc toate mesajele**
   - **Vreau sa primesc numai mesaje despre produs**
   - **Nu vreau sa primesc niciun mesaj**
4. Faceți clic pe **Creează**.
5. Faceți clic pe **Finalizează** pentru a încheia programul asistent.
6. **Activați-vă contul.** Pentru a vă putea utiliza contul, trebuie mai întâi să îl activați. Verificați-vă adresa de e-mail și urmați instrucțiunile din mesajul trimis de către serviciul de înregistrare BitDefender.

Deja am un cont BitDefender

BitDefender va detecta automat dacă ați creat anterior un cont BitDefender pe calculatorul dumneavoastră. În acest caz, furnizați parola contului dvs și faceți clic pe **Accesează**. Faceți clic pe **Finalizează** pentru a încheia programul asistent.

Dacă aveți deja un cont activ, dar BitDefender nu-l detectează, urmați pașii de mai jos pentru a înregistra produsul cu contul respectiv:

1. Selectați **Accesează cont creat anterior**.
2. Introduceți adresa de e-mail și parola contului dvs în câmpurile corespunzătoare.

   Notă
   Dacă v-ați uitat parola, faceți clic pe **V-ați uitat parola?** și urmați instrucțiunile.

3. Opțional, BitDefender vă poate informa despre oferte speciale și promoții folosind adresa de e-mail a contului dumneavoastră. Selectați una dintre opțiunile disponibile din meniu:
   - **Vreau sa primesc toate mesajele**

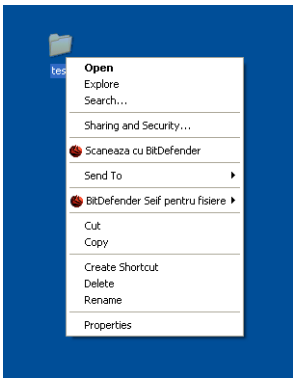
- **Vreau sa primesc numai mesaje despre produs**
- **Nu vreau sa primesc niciun mesaj**

4. Faceți clic pe **Accesează**.
5. Faceți clic pe **Finalizează** pentru a încheia programul asistent.

Integrarea în Windows și în aplicațiile terților

29. Integrarea în meniul contextual Windows

Meniul contextual Windows apare atunci când faceți clic-dreapta pe un fișier sau pe un director de pe calculator sau pe obiectele de pe desktop.



Meniul contextual Windows

BitDefender se integrează în meniul contextual Windows pentru a vă ajuta să scanați fișiere după viruși rapid și să împiedicați accesul altor utilizatori la fișierele dumneavoastră personale. Puteți găsi rapid opțiunile BitDefender în meniul contextual uitându-vă după iconița BitDefender.

- Scanează cu BitDefender
- Seiful BitDefender pentru fișiere

29.1. Scanează cu BitDefender

Utilizând meniul contextual Windows, puteți scana cu ușurință fișiere, directoare și chiar partiții întregi. Faceți clic-dreapta pe obiectul pe care doriți să-l scanați și selectați **Scanează cu BitDefender** din meniu. Va apărea programul asistent de scanare care vă va ghida de-a lungul procesului de scanare.

Opțiuni de scanare. Opțiunile de scanare sunt pre-configurate pentru a obține rata maximă de detecție. Dacă sunt detectate fișiere infectate, BitDefender va încerca să le dezinfecteze (va elimina codul malițios). Dacă dezinfectarea eșuează, programul asistent de scanare vă va permite să specificați alte acțiuni ce vor fi luate asupra fișierelor infectate.

Dacă doriți să modificați opțiunile de scanare, urmați acești pași:

1. Deschideți BitDefender și treceți interfața în Modul Expert.
2. Faceți clic pe **Antivirus** în meniul din stânga.

3. Faceți clic pe tabul **Scanare viruși**.
4. Faceți clic-dreapta pe sarcina **Scanare contextuală** și selectați **Deschide**. Va apărea o fereastră.
5. Faceți clic pe **Personalizat** și configurați opțiunile de scanare după cum este necesar. Pentru a afla ce face o opțiune, țineți mouse-ul deasupra ei și citiți descrierea afișată în partea de jos a ferestrei.
6. Faceți clic pe **OK** pentru a salva modificările.
7. Faceți clic pe **OK** pentru a confirma și aplica noile opțiuni de scanare.

Important

Este recomandat să nu modificați opțiunile de scanare ale acestei metode de scanare decât dacă aveți un motiv anume să faceți acest lucru.

29.2. Seiful BitDefender pentru fișiere

Seiful BitDefender pentru fișiere vă ajută să păstrați în siguranță pe calculator documentele dumneavoastră confidențiale prin utilizarea seifurilor de fișiere.

- Seiful de fișiere reprezintă un spațiu sigur de stocare a informațiilor personale sau a fișierelor confidențiale.
- Seiful de fișiere este de fapt un fișier criptat de pe calculatorul dumneavoastră, având extensia bvd. Seiful de fișiere fiind criptat, datele dinăuntrul acestuia sunt protejate împotriva furtului sau a altor pericole informatice.
- Atunci când deschideți acest fișier bvd, va apărea o nouă partiție logică (un nou drive). Veți înțelege mai ușor procesul prin analogie cu un proces similar: montarea unei imagini ISO ca CD virtual.

  Deschideți My Computer și veți vedea un nou drive, care corespunde seifului dumneavoastră de fișiere. Puteți face diverse operații cu fișierele din seif (copiere, ștergere, modificare etc). Fișierele sunt protejate cât timp se află în acest drive (deoarece este nevoie de parolă pentru deschiderea acestuia).

  Atunci când ați terminat ce aveați de făcut, închideți seiful pentru a proteja conținutul acestuia.

Puteți identifica rapid seifurile BitDefender de fișiere de pe calculatorul dumneavoastră după iconița BitDefender și extensia `.bvd` extension.

Notă

Această secțiune vă arată cum să creați și să administrați seifurile BitDefender de fișiere folosind numai opțiunile oferite de meniul contextual Windows. Mai puteți crea și gestiona seifurile de fișiere direct din interfața BitDefender.

- În Modul Intermediar, mergeți la tabul >Seif fișiere și folosiți opțiunile din secțiunea **Sarcini rapide**. Un program asistent vă va ajuta să finalizați fiecare sarcină.

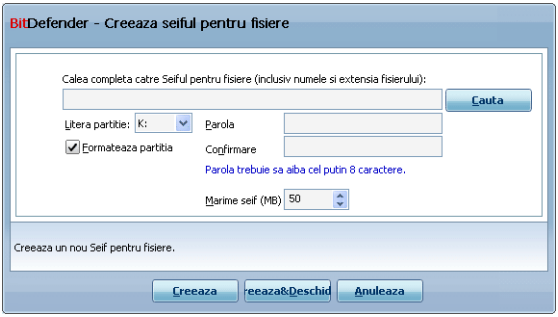
- Pentru o abordare mai directă, treceți interfața în Modul Expert și faceți clic pe **Criptare** în meniul din stânga. Pe tabul Criptare fișiere, puteți vedea și administra seifurile de fișiere existente, precum și conținutul acestora.

29.2.1. Creați seiful

Rețineți că un seif este de fapt un fișier cu extensia `.bvd`. Numai atunci când deschideți seiful va apărea o partiție virtuală în My Computer unde puteți stoca fișiere în siguranță. Când creați un seif, trebuie să specificați unde și cu ce nume să fie salvat seiful pe calculatorul dumneavoastră. De asemenea, trebuie să specificați o parolă pentru a-i proteja conținutul. Numai utilizatorii care cunosc parola pot deschide seiful și pot accesa documentele și datele stocate în acesta.

Pentru a crea un seif, urmați acești pași:

1. Faceți clic-dreapta pe desktop sau într-un director de pe calculatorul dumneavoastră, duceți cursorul deasupra opțiunii **Seif BitDefender** și selectați **Creează seif**. Va apărea următoarea fereastră:



Creare seif de fișiere

2. Specificați locația și numele seifului de fișiere.
   - Faceți clic pe **Caută**, selectați locația seifului și salvați fișierul seif cu numele dorit.
   - Tastați numele seifului în câmpul corespunzător dacă doriți să fie creat în My Documents. Pentru a deschide My Documents, faceți clic pe meniul Windows Start și apoi pe **My Documents**.
   - Introduceți calea completă pe disc a fișierului seif. De exemplu, `C:\seiful_meu.bvd`.
3. Selectați din meniu o literă pentru partiție. Atunci când deschideți seiful, puteți vedea în My Computer o partiție virtuală denumită cu litera selectată.

4. Introduceți noua parolă a seifului în câmpurile **Parolă nouă** și **Confirmare**. Oricine va încerca să deschidă seiful și să acceseze fișierele acestuia va trebui să furnizeze parola.
5. Selectați **Formatează partiția** pentru a formata partiția virtuală corespunzătoare seifului. Trebuie să formatați partiția virtuală înainte de a putea adăuga fișiere în seif.
6. Dacă doriți să modificați dimensiunea implicită (50 MB) a seifului, introduceți valoarea dorită în câmpul **Dimensiune seif**.
7. Faceți clic pe **Creează** dacă doriți doar să creați seiful în locația selectată. Pentru a crea și a afișa seiful ca partiție virtuală în My Computer, faceți clic pe **Creează&Deschide**.

BitDefender vă va informa imediat despre rezultatul operației. Dacă a avut loc o eroare, utilizați mesajul de eroare pentru a o depana. Faceți clic pe **OK** pentru a închide fereastra.

Notă

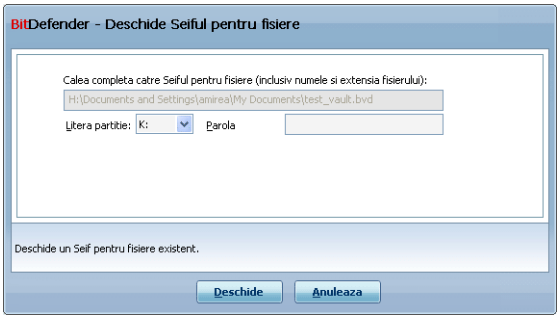
Poate fi convenabil să salvați toate seifurile de fișiere în același loc. Astfel, le veți găsi mai ușor.

29.2.2. Deschide seiful

Pentru a accesa și a lucra cu fișierele stocate într-un seif, trebuie mai întâi să deschideți seiful. Atunci când deschideți seiful, puteți vedea o partiție virtuală în My Computer. Partiția este denumită cu litera atribuită seifului.

Pentru a deschide un seif, urmați acești pași:

1. Căutați pe calculator fișierul `.bvd` reprezentând seiful pe care doriți să-l deschideți.
2. Faceți clic-dreapta pe fișier, duceți cursorul deasupra opțiunii **Seiful BitDefender pentru fișiere** și selectați **Deschide**. Mai rapid, faceți dublu-clic pe fișier, sau faceți clic-dreapta și selectați **Deschide**. Va apărea următoarea fereastră:



Deschide seif de fișiere

3. Selectați din meniu o literă pentru partiție.
4. Introduceți parola seifului în câmpul **Parolă**.
5. Faceți clic pe **Deschide**.

BitDefender vă va informa imediat despre rezultatul operației. Dacă a avut loc o eroare, utilizați mesajul de eroare pentru a o depana. Faceți clic pe **OK** pentru a închide fereastra.

29.2.3. Închide seif

Atunci când ați terminat de lucrat într-un seif de fișiere, trebuie să îl închideți pentru a vă proteja datele. Prin închiderea seifului, partiția virtuală corespunzătoare dispare din My Computer. Ca urmare, este complet blocat accesul la datele stocate în seif.

Pentru a închide un seif, urmați acești pași:

1. Deschideți My Computer (faceți clic pe meniul Windows Start și apoi pe **My Computer**).
2. Identificați partiția virtuală corespunzătoare seifului pe care doriți să-l închideți. Uitați-vă după litera pe care ați atribuit-o seifului atunci când l-ați deschis.
3. Faceți clic-dreapta pe partiția virtuală respectivă, duceți cursorul deasupra opțiunii **Seiful BitDefender pentru fișiere** și selectați **Închide**.

De asemenea, puteți face clic-dreapta pe fișierul `.bvd` reprezentând seiful, plasați cursorul pe **Seif pentru fișiere BitDefender** și faceți clic pe **Închide**.

BitDefender vă va informa imediat despre rezultatul operației. Dacă a avut loc o eroare, utilizați mesajul de eroare pentru a o depana. Faceți clic pe **OK** pentru a închide fereastra.

Notă

Dacă sunt deschise mai multe seifuri, este mai convenabil să utilizați interfața BitDefender în Modul Expert. Dacă mergeți la **Criptare**, tabul Criptare fișiere, veți vedea un tabel care oferă informații despre seifurile existente. Puteți vedea dacă seiful este deschis și, în acest caz, litera atribuită partiției virtuale.

29.2.4. Adaugă în seiful de fișiere

Înainte de a putea adăuga fișiere sau directoare într-un seif, trebuie să deschideți seiful. Odată ce un seif este deschis, puteți stoca fișiere sau directoare în interiorul acestuia, folosind meniul contextual. Faceți clic-dreapta pe fișierul sau directorul pe care doriți să-l copiați într-un seif, duceți cursorul deasupra opțiunii **Seiful BitDefender pentru fișiere** și selectați **Adaugă în seiful pentru fișiere**.

- Dacă un singur seif este deschis, fișierul sau directorul este copiat direct în acel seif.
- Dacă mai multe seifuri sunt deschise, vi se va solicita să alegeți seiful în care să fie copiat obiectul. Selectați din meniu litera corespunzătoare seifului dorit și faceți clic pe **OK** pentru a copia obiectul.

Puteți folosi, de asemenea, partiția virtuală corespunzătoare seifului. Urmați pașii:

1. Deschideți My Computer (faceți clic pe meniul Windows Start și apoi pe **My Computer**).
2. Intrați în partiția virtuală corespunzătoare seifului. Uitați-vă după litera pe care ați atribuit-o seifului atunci când l-ați deschis.
3. Copiați sau trageți fișiere și directoare direct în această partiție virtuală.

29.2.5. Elimină din seiful de fișiere

Pentru a elimina fișiere sau directoare dintr-un seif, trebuie ca seiful să fie deschis. Pentru a șterge fișiere sau directoare dintr-un seif, urmați acești pași:

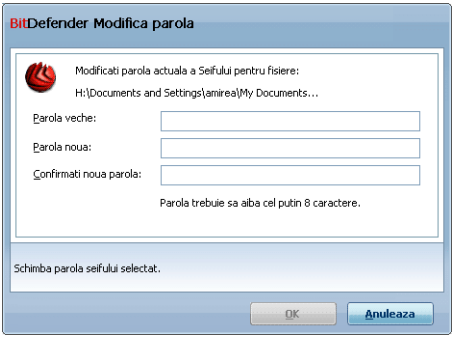
1. Deschideți My Computer (faceți clic pe meniul Windows Start și apoi pe **My Computer**).
2. Intrați în partiția virtuală corespunzătoare seifului. Uitați-vă după litera pe care ați atribuit-o seifului atunci când l-ați deschis.
3. Ștergeți fișierele sau directoarele așa cum faceți în mod normal în Windows (de exemplu, faceți clic-dreapta pe un fișier pe care doriți să îl ștergeți și selectați **Delete (Șterge)**).

29.2.6. Modificare parolă seif

Parola protejează conținutul unui seif împotriva accesului neautorizat. Numai utilizatorii care cunosc parola pot deschide seiful și pot accesa documentele și datele stocate în acesta.

Un seif trebuie să fie închis pentru a-i putea schimba parola. Pentru a schimba parola unui seif, urmați acești pași:

1. Căutați pe calculator fișierul `.bvd` reprezentând seiful.
2. Faceți clic-dreapta pe fișier, duceți cursorul deasupra opțiunii **Seiful BitDefender pentru fișiere** și selectați **Schimbă parola Seifului**. Va apărea următoarea fereastră:



Modificare parolă seif

3. Introduceți parola curentă a seifului în câmpul **Parolă veche**.
4. Introduceți noua parolă a seifului în câmpurile **Parolă nouă** și **Confirmă noua parolă**.

> **Notă**
>
> Parola trebuie să conțină minim 8 caractere. Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @).

5. Faceți clic pe **OK** pentru a salva parola.

BitDefender vă va informa imediat despre rezultatul operației. Dacă a avut loc o eroare, utilizați mesajul de eroare pentru a o depana. Faceți clic pe **OK** pentru a închide fereastra.

30. Integrarea cu browserele web

BitDefender vă protejează împotriva tentativelor de phishing atunci când navigați pe Internet. Acesta scanează paginile web accesate și vă alertează dacă sunt amenințări phishing. O listă albă de pagini web care nu vor fi scanate de BitDefender poate fi configurată.

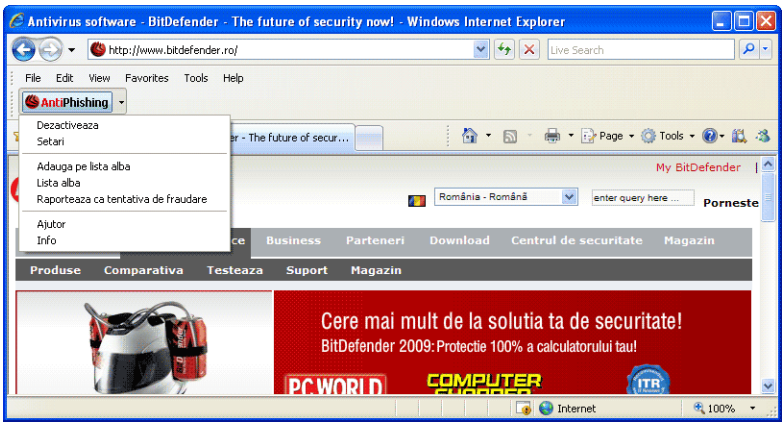
BitDefender se integrează direct, printr-o bară de comenzi intuitivă și ușor de folosit, cu următoarele browsere web:

- Internet Explorer
- Mozilla Firefox

Puteți administra ușor și eficient protecția antiphishing și lista albă utilizând bara de comenzi BitDefender Antiphishing integrată în browserele web de mai sus.

Bara de comenzi antiphishing, reprezentată prin iconița BitDefender se află în zona de sus a browserului. Faceți clic pe ea pentru a deschide meniul barei de instrumente.

Notă
Dacă nu puteți vedea bara de instrumente, deschideți meniul **View**, mergeți cu cursorul pe **Toolbars** și bifați **BitDefender Toolbar**.



Bara de comenzi antiphishing

Următoarele comenzi sunt disponibile pe meniul barei de instrumente:

- **Activează / Dezactivează** - activează / dezactivează protecția antiphishing BitDefender în browserul web curent.

- **Setări** - deschide o fereastră în care puteți specifica setările barei de comenzi antiphishing. Următoarele opțiuni sunt disponibile:
  - **Protecția antiphishing pentru web în timp real** - detectează și vă avertizează în timp real dacă un site web este folosit pentru a fura informații personale. Această opțiune controlează protecția antiphishing oferită de BitDefender doar pentru browserul web curent.
  - **Întreabă înainte de a adăuga în lista albă** - vă avertizează înainte de a adăuga o pagină web în lista albă.
- **Adaugă pe lista albă** - adaugă pagina web curentă în lista albă.

Notă

Adăugarea unei pagini web în lista albă înseamnă că BitDefender nu o va mai scana după amenințări phishing. Vă recomandăm să adăugați în lista albă doar paginile web în care aveți deplină încredere.

- **Lista albă** - deschide lista albă.

Lista albă antiphishing

Puteți vedea lista tuturor paginilor web care nu sunt verificate de motoarele antiphishing ale BitDefender. Dacă doriți să ștergeți o pagină web din lista albă, astfel încât să fiți avertizat în legătură cu orice amenințare phishing existentă pe pagina respectivă, faceți clic pe butonul **Șterge** corespunzător paginii.

Puteți adăuga paginile web în care aveți deplină încredere pe lista albă pentru a nu mai fi scanate de motoarele antiphishing. Pentru a adăuga o pagină web pe lista albă, introduceți adresa acesteia în câmpul corespunzător și faceți clic pe **Adaugă**.

- **Raportează ca fraudat (phishing)** - informează laboratorul BitDefender că site-ul web respectiv este folosit pentru furt de informații personale. Raportând site-urile web folosite pentru fraudă, ajutați la protejarea altor persoane împotriva furtului de identitate.
- **Ajutor** - deschide documentația electronică.
- **Despre** - deschide o fereastră în care puteți vedea informații despre BitDefender și unde să apelați pentru ajutor în cazul unei probleme.

31. Integrarea în clienți de mesagerie instant

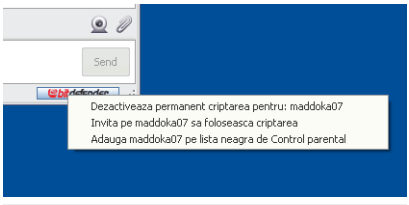
BitDefender oferă capabilități de criptare pentru a vă proteja documentele confidențiale și conversațiile dumneavoastră prin mesageria instant, prin Yahoo Messenger și MSN Messenger.

În mod implicit, BitDefender criptează toate sesiunile dumneavoastră de chat prin mesagerie instant cu condiția ca:

- Partenerul dumneavoastră de chat are instalată o versiune de BitDefender care suportă criptarea mesageriei instant (IM), iar Criptarea IM este activată pentru aplicația de mesagerie instant folosită pentru chat.
- Atât dumneavoastră, cât si partenerul dumneavoastră de chat, să utilizați fie Yahoo Messenger, fie Windows Live (MSN) Messenger.

Important
BitDefender nu va cripta o conversație dacă un partener de chat folosește o aplicație web pentru chat, cum ar fi Meebo, sau o altă aplicație de chat care suportă Yahoo Messenger sau MSN.

Puteți configura ușor criptarea mesageriei instant folosind bara de comenzi BitDefender din fereastra de chat. Bara de comenzi se găsește în mod normal în colțul din dreapta-jos al ferestrei de chat. Uitați-vă după logo-ul BitDefender pentru a o găsi.



Bara de comenzi BitDefender

Notă
Bara de comenzi arată când o conversație este criptată prin afișarea unei cheițe 🗝 lângă logo-ul BitDefender.

Făcând clic pe bara de comenzi BitDefender, vă sunt oferite următoarele opțiuni:

- **Dezactivează permanent criptarea pentru contact.**
- **Invită pe contact să utilizeze criptarea.** Pentru a cripta conversația, contactul dumneavoastră trebuie să instaleze BitDefender și să utilizeze un program de mesagerie instant compatibil.
- **Adaugă pe contact în lista neagră a controlului parental.** Dacă adăugați un contact în lista neagră a controlului parental și controlul parental este activat, nu veți mai vedea mesajele instant trimise de contactul respectiv. Pentru a elimina contactul din lista neagră, faceți clic pe bara de comenzi și selectați **Elimină pe contact din lista neagră a controlului parental**.

32. Integrarea cu clienții de mail

BitDefender Internet Security 2010 include un modul Antispam. Antispam verifică mesajele e-mail pe care le primiți și le identifică pe cele care sunt nesolicitate (spam). Mesajele spam detectate de BitDefender sunt marcate cu prefixul [SPAM] în subiect.

Notă
Protecția antispam este oferită pentru toți clienții de mail POP3/SMTP.

BitDefender se integrează direct, printr-o bară de comenzi intuitivă și ușor de folosit, cu următorii clienți de mail:

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

BitDefender mută în mod automat mesajele spam într-un anumit director, după cum urmează:

- În Microsoft Outlook, mesajele spam sunt mutate într-un director **Spam**, situat în directorul **Deleted Items**. Directorul **Spam** este creat în timpul instalării BitDefender.
- În Outlook Express și Windows Mail, mesajele spam sunt mutate direct în **Deleted Items**.
- În Mozilla Thunderbird, mesajele spam sunt mutate într-un director **Spam**, situat în directorul **Trash**. Directorul **Spam** este creat în timpul instalării BitDefender.

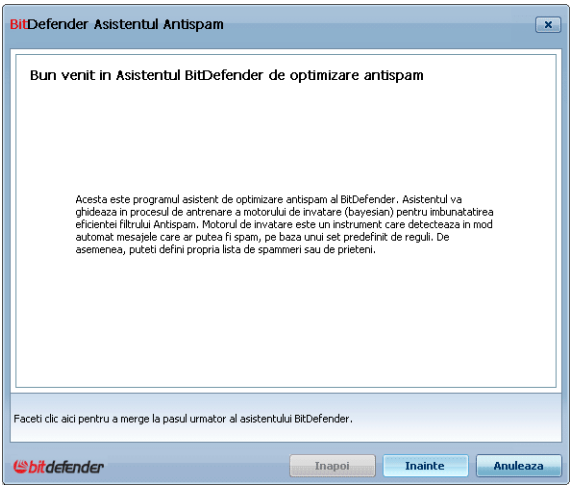
Dacă utilizați alt client de mail, trebuie să creați o regulă pentru a muta mesajele e-mail marcate [SPAM] de BitDefender într-un anumit director de carantină.

32.1. Asistentul de configurare Antispam

Prima dată când rulați clientul dumneavoatră de mail după instalarea BitDefender, va apărea un program asistent care vă va ajuta să configurați lista de prieteni și lista de spammeri și să educați motorul de învățare (bayesian) pentru a crește eficiența filtrelor Antispam.

Notă
Programul asistent mai poate fi lansat, oricând doriți, făcând clic pe butonul **Asistent** din bara de comenzi Antispam.

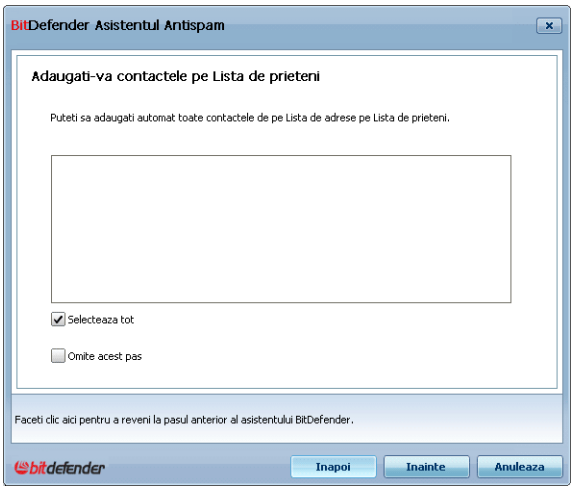
32.1.1. Pasul 1/6 - Fereastră de întâmpinare



Fereastra de întâmpinare

Faceți clic pe **Înainte**.

32.1.2. Pasul 2/6 - Completați lista de prieteni



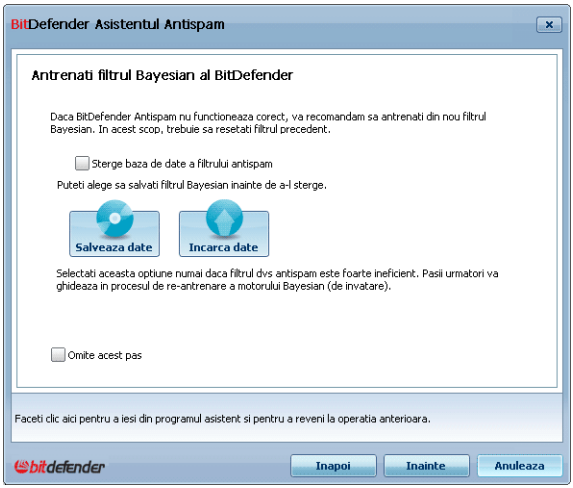
Completați lista de prieteni

Aici puteți vedea toate adresele din **Address Book**. Selectați-le pe cele pe care doriți să le adăugați la **lista de prieteni** (vă recomandăm să le selectați pe toate). Veți primi toate mesajele de la aceste adrese, indiferent de conținut.

Pentru a vă adăuga toate contactele pe lista de prieteni, bifați **Selectează tot**.

Dacă doriți să săriți peste acest pas al configurării, selectați **Sari peste acest pas**. Faceți clic pe **Înainte** pentru a continua.

32.1.3. Pasul 3/6 - Șterge baza de date Bayesiană



Șterge baza de date Bayesiană

Există posibilitatea să descoperiți că filtrul Antispam a început să-și piardă eficiența. Aceasta se poate întâmpla din cauza educării incorecte (ați etichetat din greșeală unele mesaje legitime ca Spam, sau invers). Dacă filtrul este ineficient, trebuie să ștergeți baza de date a filtrului și să reeducați filtrul urmând pașii acestui program asistent.

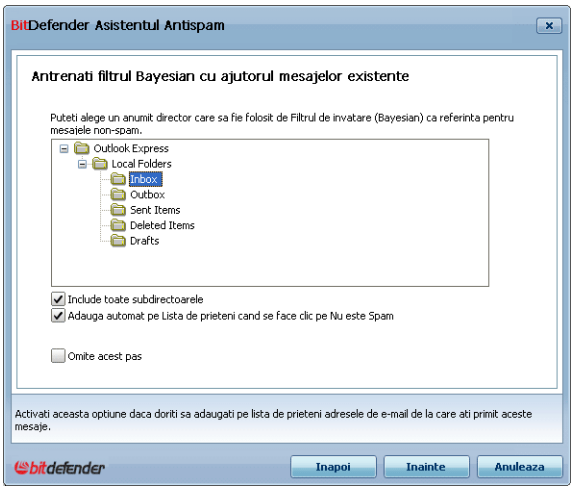
Selectați **Șterge baza de date a filtrului antispam** dacă doriți să ștergeți baza de date a Filtrului Bayesian.

Puteți salva baza de date a filtrului Bayesian într-un fișier pentru a o putea folosi împreună cu un alt produs BitDefender sau după reinstalarea BitDefender. Pentru a salva baza de date Bayesiană, faceți clic pe butonul **Salvează Bayes** și salvați-o în locația dorită. Fișierul va avea o extensie `.dat`.

Pentru a încărca o bază de date Bayesiană salvată anterior, faceți clic pe butonul **Încărcă Bayes** și deschideți fișierul corespunzător.

Dacă doriți să săriți peste acest pas al configurării, selectați **Sari peste acest pas**. Faceți clic pe **Înainte** pentru a continua.

32.1.4. Pasul 4/6 - Educați filtrul Bayesian cu mesaje legitime



Educați filtrul Bayesian cu mesaje legitime

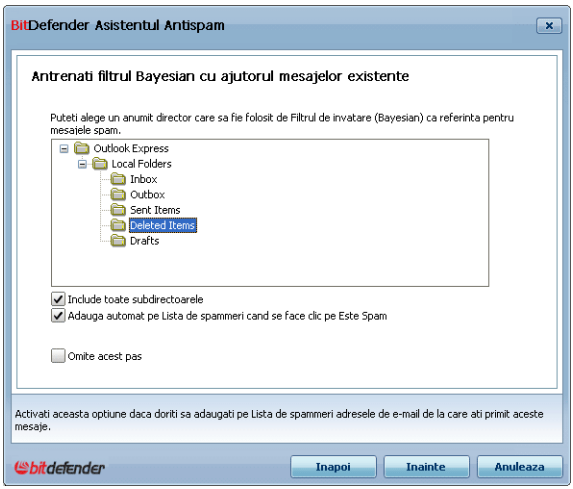
Selectați un director care conține mesaje e-mail legitime. Aceste mesaje vor fi folosite pentru a educa filtrul Antispam.

Sub lista de directoare se găsesc două opțiuni avansate:

- **Include toate subdirectoarele** - pentru a include subdirectoarele în selecție.
- **Adaugă automat pe lista de prieteni** - pentru a adăuga expeditorii pe lista de prieteni.

Dacă doriți să săriți peste acest pas al configurării, selectați **Sari peste acest pas**. Faceți clic pe **Înainte** pentru a continua.

32.1.5. Pasul 5/6 - Educați filtrul Bayesian cu SPAM



Educați filtrul Bayesian cu SPAM

Selectați un director care conține mesaje Spam. Aceste mesaje vor fi folosite pentru a educa filtrul Antispam.

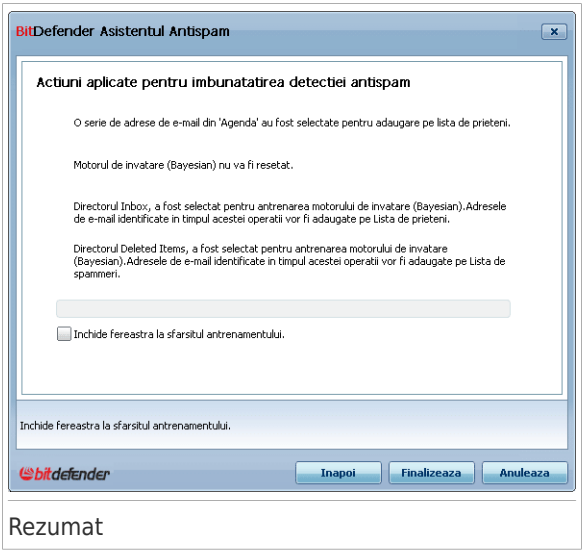
Important
Directorul nu trebuie să conțină niciun mesaj legitim, altfel performanțele filtrului Antispam vor fi considerabil reduse.

Sub lista de directoare se găsesc două opțiuni avansate:

- **Include toate subdirectoarele** - pentru a include subdirectoarele în selecție.
- **Adaugă automat pe lista de spammeri** - pentru a adăuga expeditorii pe lista de spammeri. Mesajele e-mail de la acești expeditori vor fi marcate ca spam întotdeauna și prelucrate în consecință.

Dacă doriți să săriți peste acest pas al configurării, selectați **Sari peste acest pas**. Faceți clic pe **Înainte** pentru a continua.

32.1.6. Step 6/6 - Sumar



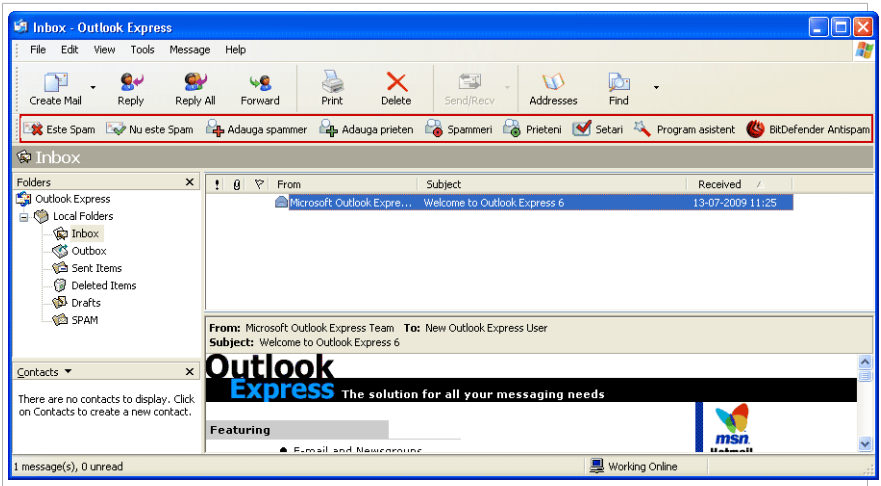
Rezumat

În această fereastră puteți vedea toate setările făcute în programul asistent. Puteți face orice schimbări, revenind la pașii anteriori (faceți clic pe **Înapoi**).

Dacă nu doriți să faceți nici o modificare, faceți clic pe **Finalizare** pentru a închide programul asistent.

32.2. Bara de comenzi BitDefender

În partea de sus a ferestrei clientului dumneavoastră de mail, puteți vedea bara de comenzi antispam. Bara de comenzi antispam vă ajută să administrați protecția antispam direct din clientul dumneavoastră de mail. Puteți corecta BitDefender cu ușurință dacă acesta a marcat un mesaj legitim ca SPAM.



Bara de comenzi BitDefender

Fiecare buton al barei de comenzi este explicat mai jos:

- **Este Spam** - trimite un mesaj modulului Bayesian indicând că mesajul selectat este Spam. Mesajul va primi eticheta SPAM și va fi mutat în directorul**Spam**.

  Mesajele viitoare care seamănă cu acest mesaj vor fi considerate SPAM.

  Notă
  Puteți selecta unul sau mai multe mesaje.

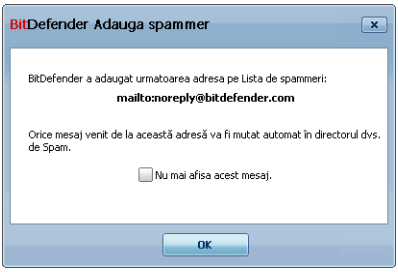
- **Nu este Spam** - trimite un mesaj către modulul Bayesian cu precizarea că mesajul selectat nu este spam, iar BitDefender nu ar fi trebuit să-l marcheze. E-mail-ul va fi mutat din directorul **Spam** în directorul **Primite**.

  Mesajele viitoare care seamănă cu acesta nu vor mai fi considerate SPAM.

  Notă
  Puteți selecta unul sau mai multe mesaje.

  Important
  Butonul **Nu este Spam** este activ doar când selectați un mesaj etichetat ca SPAM de către BitDefender (în mod normal aceste mesaje se găsesc în directorul **Spam**).

- **Adaugă Spammer** - Adaugă expeditorul e-mail-ului selectat pe lista de spammeri.



Adaugă spamer

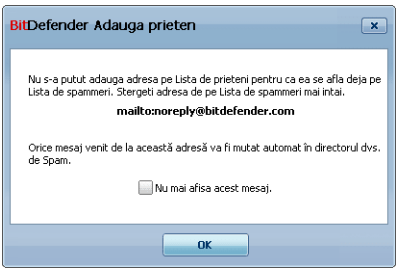
Selectați **Nu mai afișa acest mesaj** dacă nu doriți să vi se ceară confirmarea în momentul adăugării expeditorului pe lista de prieteni.

Faceți clic pe **OK** pentru a închide fereastra.

Viitoarele mesaje primite de la adresa respectivă vor fi etichetate ca SPAM.

Notă
Puteți selecta câți expeditori doriți.

- **Adaugă prieten** - Adaugă expeditorul e-mail-ului selectat pe lista de prieteni.



Adaugă prieten

Selectați **Nu mai afișa acest mesaj** dacă nu doriți să vi se ceară confirmarea în momentul adăugării expeditorului pe lista de prieteni.

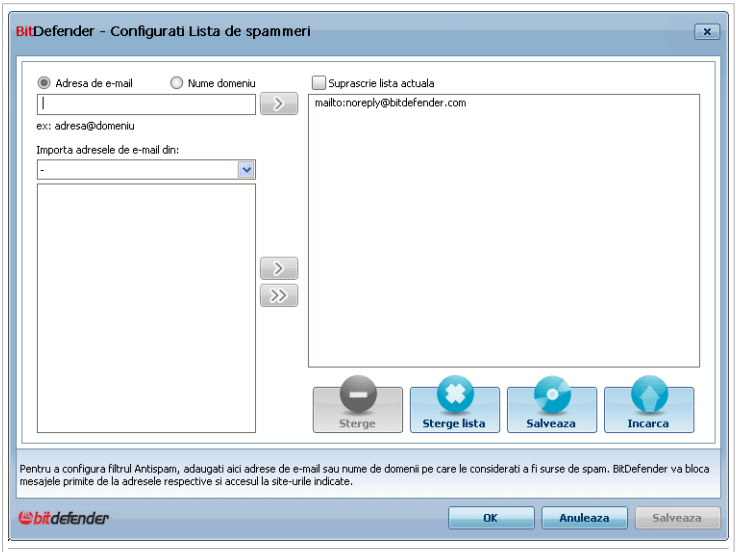
Faceți clic pe **OK** pentru a închide fereastra.

Veți primi toate mesajele de la această adresă, indiferent de conținutul lor.

Notă
Puteți selecta câți expeditori doriți.

- **Spammeri** - deschide **lista de spammeri** care conține adrese de e-mail de la care nu doriți să primiți mesaje, indiferent de conținutul acestora.

Notă
Orice mesaj primit de la o adresă din **lista de spammeri** va fi automat etichetat ca Spam, fără altă procesare.



Lista de spammeri

Aici puteți adăuga sau șterge intrări din **lista de spammeri** .

Dacă doriți să adăugați o adresă, selectați **E-mail** scrieți adresa și faceți clic pe butonul . Adresa va apărea în **lista de spammeri**.

Important
Sintaxă: name@domain.com.

Dacă doriți să adăugați un domeniu, selectați **Domeniul**, scrieți numele domeniului si faceți clic pe butonul . Domeniul va apărea în **lista de spammeri**.

Important
Sintaxă:
- @domain.com, *domain.com and domain.com - - toate mesajele primite de la domain.com vor fi etichetate ca SPAM;
- *domain* - toate mesajele primite de la domain(indiferent de sufixul domeniului) vor fi etichetate ca SPAM;
- *com - a- toate mesajele primite având sufixul domeniului com vor fi etichetate ca SPAM.

Avertisment

Nu adăugați nume de domenii legitime ale unor servicii de e-mail bazate pe web (Yahoo, Gmail, Hotmail sau altele asemenea) pe Lista de spammeri. În caz contrar, mesajele e-mail primite de la orice utilizator înregistrat al unui astfel de serviciu vor fi detectate ca spam. Dacă, de exemplu, adăugați `yahoo.com` pe Lista de spammeri, toate mesajele e-mail care provin de la adrese `yahoo.com` vor fi marcate ca `[spam]`.

Pentru a importa adrese e-mail din **Windows Address Book**/**Outlook Express Folders** în **Microsoft Outlook** / **Outlook Express** / **Windows Mail**, selectați opțiunea corespunzătoare din meniul **Importă adrese de mail din**.

În cazul selectării **Microsoft Outlook Express** / **Windows Mail** va apărea o nouă fereastră, de unde veți putea selecta directorul ce conține adresele e-mail pe care doriți să le adăugați la **lista de spammeri**. Alegeți-le și faceți clic pe **Selectează**.

În ambele cazuri adresele de e-mail vor apărea în lista pentru importare. Selectați-le pe cele dorite și faceți clic pe pentru a le adăuga la **lista de spammeri**. Dacă faceți clic pe toate adresele vor fi adăugate în listă.

Pentru a șterge un obiect de pe listă, selectați-l și faceți clic pe butonul **Șterge**. Pentru a șterge toate înregistrările de pe listă faceți clic pe butonul **Șterge jurnal** și apoi pe **Da**, pentru confirmare.

Puteți salva Lista de spammeri într-un fișier astfel încât s-o puteți folosi pe un alt calculator sau după reinstalarea produsului. Pentru a salva Lista de spammeri, faceți clic pe butonul **Salvează** și salvați-o în locația dorită. Fișierul va avea o extensie `.bwl`.

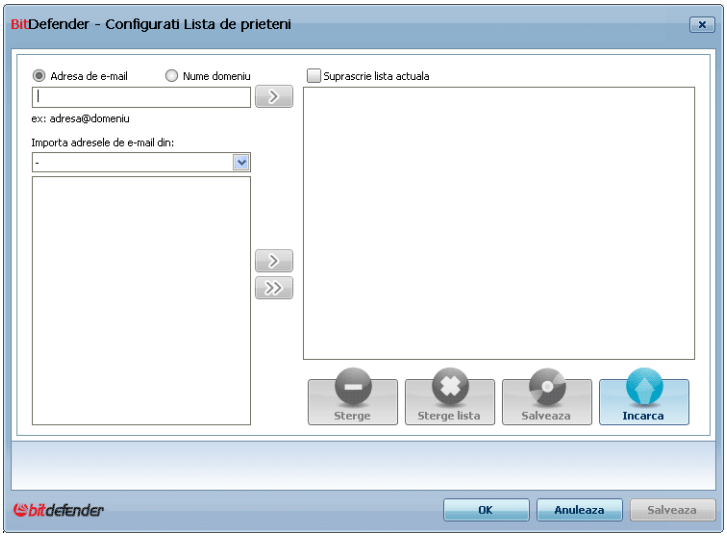
Pentru a încărca o Listă de spammeri salvată anterior, faceți clic pe butonul **Încărca** și deschideți fișierul `.bwl` corespunzător. Pentru a reseta conținutul listei curente atunci când încărcați o listă salvată anterior selectați **Suprascrie lista curentă**.

Faceți clic pe **Salvează**și**OK** pentru a salva modificările și a închide **Lista de spammeri**.

- **Prieteni** - deschide **lista de prieteni** care conține adrese de e-mail de la care doriți întotdeauna să primiți mesaje, indiferent de conținutul acestora.

Notă

Orice mesaj venit de la o adresă inclusă în **lista de prieteni** va fi trimis automat în directorul Inbox, fără a mai fi procesat.



Lista de prieteni

Aici puteți adăuga sau șterge intrări din **lista de prieteni**.

Dacă doriți să adăugați o adresă, selectați opțiunea **E-mail**, scrieți adresa și faceți clic pe butonul . Adresa va apărea în **lista de prieteni**.

Important
Sintaxă: name@domain.com.

Dacă doriți să adăugați un domeniu, selectați **Domeniul**, scrieți numele domeniului și faceți clic pe butonul . Domeniul va apărea în **lista de prieteni**.

Important
Sintaxă:

- @domain.com, *domain.com și domain.com - toate mesajele primite de la domain.com vor ajunge în directorul **Inbox** indiferent de conținut;
- *domain* - toate mesajele primite de la domain (indiferent de sufixul domeniului) vor ajunge în directorul **Inbox** indiferent de conținut;
- *com - toate mesajele primite având sufixul domeniului com vor ajunge în directorul **Inbox** indiferent de conținut;

Pentru a importa adrese e-mail din **Windows Address Book**/**Outlook Express Folders** în **Microsoft Outlook** / **Outlook Express** / **Windows Mail**, selectați opțiunea corespunzătoare din meniul **Importă adrese de mail din**.

Pentru **Microsoft Outlook Express / Windows Mail** va apărea o nouă fereastră din care puteți selecta directorul în care se află adresele de e-mail pe care doriți să le adăugați la **lista de prieteni**. Alegeți adresele dorite și faceți clic pe **Selectează**.

În ambele cazuri adresele de e-mail vor apărea în lista pentru importare. Selectați-le pe cele dorite și faceți clic pe pentru a le adăuga la **lista de prieteni**. Dacă faceți clic pe toate adresele vor fi adăugate în listă.

Pentru a șterge un obiect de pe listă, selectați-l și faceți clic pe butonul **Șterge**. Pentru a șterge toate înregistrările de pe listă faceți clic pe butonul **Șterge jurnal** și apoi pe **Da**, pentru confirmare.

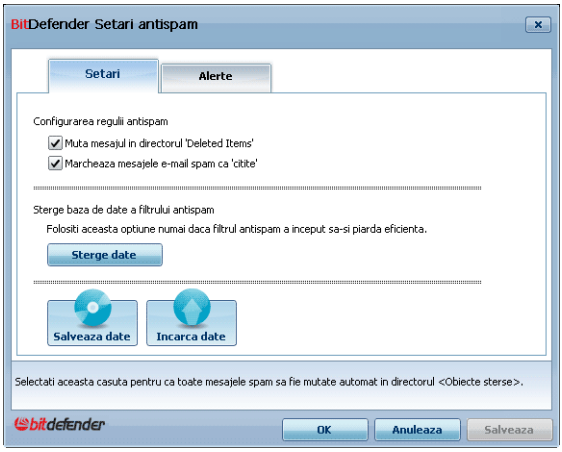
Puteți salva Lista de prieteni într-un fișier, astfel încât s-o puteți folosi pe un alt calculator sau după reinstalarea produsului. Pentru a salva Lista de prieteni, faceți clic pe butonul **Salvează** și salvați-o în locația dorită. Fișierul va avea o extensie `.bwl`.

Pentru a încărca o Listă de prieteni salvată anterior, faceți clic pe butonul **Încărca** și deschideți fișierul `.bwl` corespunzător. Pentru a reseta conținutul listei curente atunci când încărcați o listă salvată anterior selectați **Suprascrie lista curentă**.

Notă
Vă recomandăm să adăugați numele și adresele prietenilor la **lista de prieteni**.BitDefender nu va bloca mesajele de la cei de pe listă; deci adăugând prietenii vă veți asigura că mesajele legitime vor ajunge în Inbox.

Faceți clic pe **Salvează** și **OK** pentru a salva modificările și a închide **Lista de prieteni**.

- **Setări** - deschide fereastra de **Setări** unde puteți specifica unele opțiuni pentru modulul **Antispam**.



Setări

Următoarele opțiuni sunt disponibile:

- **Mută mesajul in directorul Deleted Items** - mută mesajele Spam în directorul **Deleted Items** (doar pentru Microsoft Outlook Express / Windows Mail);
- **Marchează mesajul ca 'citit'** - marchează toate mesajele Spam ca fiind citite pentru a nu fi deranjat când sosesc noi mesaje Spam.

Dacă filtrul dumneavoastră Antispam nu mai este eficient, este necesar să ștergeți baza de date a filtrului și să reeducați Filtrul Bayesian. Faceți clic pe **Șterge baza de date antispam** to reset the baza de date Bayesiană.

Puteți salva baza de date a filtrului Bayesian într-un fișier pentru a o putea folosi împreună cu un alt produs BitDefender sau după reinstalarea BitDefender. Pentru a salva baza de date Bayesiană, faceți clic pe butonul **Salvează Bayes** și salvați-o în locația dorită. Fișierul va avea o extensie `.dat`.

Pentru a încărca o bază de date Bayesiană salvată anterior, faceți clic pe butonul **Încărcă Bayes** și deschideți fișierul corespunzător.

Faceți clic pe tabul **Alerte** dacă doriți să accesați secțiunea în care puteți dezactiva apariția ferestrelor de confirmare pentru butoanele **Adaugă spammer** și **Adaugă prieten**.

Notă

În fereastra **Alerte** puteți de asemenea să activați/dezactivați apariția alertei **Selectați un mesaj email**. Această alertă apare atunci când selectați un grup în loc de un mesaj email.

- **Asistent** - deschide asistentul de configurare antispam, care vă va permite să antrenați Filtrul Bayesian pentru a spori eficiența procesului de filtrare Antispam al BitDefender. De asemenea, puteți adăuga adresele din Agenda dvs pe Lista de prieteni/spammeri.
- **BitDefender Antispam** - deschide interfața BitDefender.

Ghid de instrucțiuni

33. Cum scanați fișiere și directoare

Scanarea cu BitDefender este ușoară și flexibilă. Sunt 4 metode de a seta BitDefender să scaneze fișiere și directoare după viruși și alte aplicații malițioase:

- Utilizând meniul contextual Windows
- Utilizând sarcini de scanare
- Utilizând opțiunea Scanare manuală BitDefender
- Utilizând bara de scanare

Imediat ce ați inițiat o scanare, va apărea programul asistent de scanare care vă va ghida de-a lungul acestui proces. Pentru informații detaliate despre acest program asistent, consultați secțiunea *„Programul asistent de scanare"* (p. 57).

33.1. Utilizând meniul contextual Windows

Aceasta este metoda cea mai ușoară și recomandată pentru a scana un fișier sau un director de pe calculatorul dumneavoastră. Faceți clic-dreapta pe obiectul pe care doriți să-l scanați și selectați **Scanează cu BitDefender** din meniu. Urmați programul asistent de scanare pentru a finaliza scanarea.

Iată câteva situații în care este recomandată folosirea acestei metode de scanare:

- Suspectați un anumit fișier sau director că este infectat.
- Atunci când descărcați de pe Internet fișiere care credeți că ar putea fi periculoase.
- Scanați un director comun din rețea înainte de a copia fișiere din acesta pe calculatorul dumneavoastră.

33.2. Utilizând sarcini de scanare

Dacă doriți să vă scanați calculatorul sau anumite directoare în mod regulat, este indicat să utilizați sarcini de scanare. Sarcinile de scanare specifică locațiile care trebuie scanate de BitDefender, precum și opțiunile de scanare și acțiunile care trebuie aplicate. În plus, aveți posibilitatea să le programați pentru a fi executate în mod regulat sau la o anumită oră.

Pentru a vă scana calculatorul utilizând sarcini de scanare, trebuie să deschideți BitDefender și să rulați sarcina de scanare dorită. Pașii de urmat pentru rularea sarcinii de scanare variază în funcție de modul de vizualizare a interfeței cu utilizatorul.

Rularea sarcinilor de scanare în Modul Novice

În Modul Novice, puteți rula numai scanarea standard a întregului sistem, dacă faceți clic pe **Scanează acum**. Urmați programul asistent de scanare pentru a finaliza scanarea.

Rularea sarcinilor de scanare în Modul Intermediar

În Modul Intermediar puteți rula o serie de sarcini de scanare preconfigurate. De asemenea, puteți configura și rula sarcini de scanare personalizate în anumite locații de pe calculatorul dvs, folosind opțiunile de scanare personalizată. Urmați acești pași pentru a rula o sarcină de scanare în Modul Intermediar:

1. Faceți clic pe tabul **Securitate**.
2. În partea stângă a zonei Sarcini rapide, faceți clic pe **Scanare de sistem** pentru a lansa o scanare standard a întregului calculator. Pentru a rula o altă sarcină de scanare, faceți clic pe săgeata de pe buton și selectați sarcina de scanare dorită. Pentru a configura și executa o scanare personalizată, faceți clic pe **Scanare personalizată** . Acestea sunt sarcinile de scanare disponibile:

Sarcină de scanare	Descriere
Scanare de sistem	Scanează întregul sistem, cu excepția arhivelor. În configurația implicită, scanează după toate tipurile de aplicații periculoase, altele decât cele de tip rootkit.
Scanare profundă sistem	Scanează întregul sistem. În configurația implicită, se scanează după toate tipurile de aplicații malițioase care amenință securitatea sistemului dumneavoastră, cum ar fi virușii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) și altele.
Scanează documente	Utilizați această sarcină pentru a scana directoare importante ale utilizatorului curent: `My Documents`, `Desktop` și `StartUp`. Astfel, veți asigura siguranța documentelor dumneavostră, un spațiu de lucru sigur și rularea la pornirea sistemului a unor aplicații necompromise.
Scanare personalizată	Această opțiune vă ajută să configurați și să rulați o sarcină de scanare personalizată, permițându-vă să specificați obiectele de scanat și opțiunile generale de scanare. Puteți salva sarcini de scanare personalizată pentru a le putea accesa ulterior în Modul Intermediar sau Expert.

3. Urmați programul asistent de scanare pentru a finaliza scanarea. Dacă ați ales să efectuați o scanare personalizată, trebuie să parcurgeți programul Asistent scanare personalizată.

Rularea sarcinilor de scanare în Modul Expert

În Modul Expert, puteți rula toate sarcinile de scanare preconfigurate și, de asemenea, puteți schimba opțiunile lor de scanare. În plus, puteți crea sarcini de scanare personalizate pentru a scana anumite locații de pe calculator. Urmați acești pași pentru a rula o sarcină de scanare în Modul Expert:

1. Faceți clic pe **Antivirus** în meniul din stânga.
2. Faceți clic pe tabul **Scanare viruși**. Aici găsiți o serie de sarcini de scanare standard și puteți crea propriile sarcini de scanare. Acestea sunt sarcinile de scanare standard pe care le puteți utiliza:

Sarcină implicită	Descriere
Scanare profundă sistem	Scanează întregul sistem. În configurația implicită, se scanează după toate tipurile de aplicații malițioase care amenință securitatea sistemului dumneavoastră, cum ar fi virușii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) și altele.
Scanare de sistem	Scanează întregul sistem, cu excepția arhivelor. În configurația implicită, scanează după toate tipurile de aplicații periculoase, altele decât cele de tip rootkit.
Scanare rapidă sistem	Scanează directoarele `Windows` și `Program Files`. În configurația implicită, se scanează după toate tipurile de aplicații malițioase, mai puțin cele ascunse (rootkituri), dar nu sunt scanate memoria, regiștrii și fișierele cookie.
Documentele mele	Utilizați această sarcină pentru a scana directoare importante ale utilizatorului curent: `My Documents`, `Desktop` și `StartUp`. Astfel, veți asigura siguranța documentelor dumneavoastră, un spațiu de lucru sigur și rularea la pornirea sistemului a unor aplicații necompromise.

3. Faceți dublu-clic pe sarcina de scanare pe care doriți să o rulați.
4. Urmați programul asistent de scanare pentru a finaliza scanarea.

33.3. Utilizând opțiunea Scanare manuală BitDefender

Opțiunea Scanare manuală BitDefender vă permite să scanați un anumit director sau partiție de hard-disc, fără a crea o sarcină de scanare. Această funcționalitate a fost concepută pentru a fi utilizată atunci când Windows funcționează în Safe Mode. Dacă sistemul dumneavoastră este infectat cu un virus rezistent (care nu poate fi eliminat în urma unei scanări normale), puteți încerca să eliminați virusul pornind Windows în Safe Mode și scanând fiecare partiție de hard-disc folosind opțiunea Scanare manuală BitDefender.

Pentru a vă scana calculatorul utilizând opțiunea Scanare manuală BitDefender, urmați acești pași:

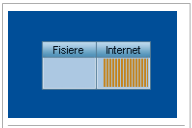
1. Pe meniul Windows Start  , urmați calea **Start → Programs → BitDefender 2010 → Scanare manuală BitDefender**. Va apărea o nouă fereastră.
2. Faceți clic pe **Adaugă director** pentru a selecta ținta scanării. Va apărea o nouă fereastră.
3. Selectați locația de scanat:
   - Pentru a vă scana desktopul, selectați **Desktop**.
   - Pentru a scana o partiție de hard-disc, selectați partiția respectivă din My Computer.
   - Pentru a scana un anumit director, căutați și selectați directorul respectiv.
4. Faceți clic pe **OK**.
5. Faceți clic pe **Continue** pentru a începe scanarea.
6. Urmați programul asistent de scanare pentru a finaliza scanarea.

Ce este Safe Mode?
Safe Mode este un mod special de a porni Windows, utilizat în principal pentru a depana problemele care afectează funcționarea normală a Windows. Aceste probleme variază de la conflicte provocate de drivere până la viruși care împiedică pornirea normală a Windows. În Safe Mode, Windows încarcă doar un minim de componente ale sistemului de operare și drivere de bază. Doar câteva aplicații funcționează în Safe Mode. Acesta este motivul pentru care majoritatea virușilor sunt inactivi și pot fi ușor eliminați atunci când Windows operează în Safe Mode.
Pentru a porni Windows în Safe Mode, reporniți calculatorul și apăsați tasta F8 încontinuu până apare meniul de opțiuni avansate al Windows (Windows Advanced Options Menu). Puteți alege între mai multe opțiuni de a porni Windows în Safe Mode. Este recomandat să selectați **Safe Mode with Networking** pentru a avea acces la Internet.

Notă

Pentru mai multe informații despre Safe Mode, consultați Centrul de Ajutor și Asistență al Windows (în meniul Start, faceți clic pe **Help and Support**). De asemenea, puteți găsi informații utile pe Internet.

33.4. Utilizarea barei de scanare



Bara de scanare

Bara de scanare este o reprezentare grafică a activității de scanare din sistemul dumneavoastră. Această fereastră mică este disponibilă, implicit, numai în Modul Expert.

Puteți utiliza bara de scanare pentru a scana rapid fișiere și directoare. Trageți fișierul sau directorul care doriți să fie scanat peste bara de scanare. Urmați programul asistent de scanare pentru a finaliza scanarea.

Notă
Pentru mai multe informații, consultați secțiunea *„Bara de scanare”* (p. 33).

34. Cum să programați scanarea calculatorului

Este recomandat să vă scanați calculatorul periodic pentru a-l proteja de viruși. BitDefender vă permite să programați sarcini de scanare, astfel încât să vă puteți scana automat calculatorul.

Pentru a programa BitDefender să vă scaneze calculatorul, urmați acești pași:

1. Deschideți BitDefender și treceți interfața în Modul Expert.
2. Faceți clic pe **Antivirus** în meniul din stânga.
3. Faceți clic pe tabul **Scanare viruși**. Aici găsiți o serie de sarcini de scanare standard și puteți crea propriile sarcini de scanare.
   - Sarcinile de sistem sunt disponibile și pot fi rulate pe orice cont de utilizator Windows.
   - Sarcinile de utilizator sunt disponibile și pot fi rulate numai de către utilizatorul care le-a creat.

   Acestea sunt sarcinile de scanare standard pe care le puteți programa:

Sarcină implicită	Descriere
Scanare profundă sistem	Scanează întregul sistem. În configurația implicită, se scanează după toate tipurile de aplicații malițioase care amenință securitatea sistemului dumneavoastră, cum ar fi virușii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) și altele.
Scanare de sistem	Scanează întregul sistem, cu excepția arhivelor. În configurația implicită, scanează după toate tipurile de aplicații periculoase, altele decât cele de tip rootkit.
Scanare rapidă sistem	Scanează directoarele `Windows` și `Program Files`. În configurația implicită, se scanează după toate tipurile de aplicații malițioase, mai puțin cele ascunse (rootkituri), dar nu sunt scanate memoria, regiștrii și fișierele cookie.
Scanare autologon	Scanează obiectele executate atunci când un utilizator se conectează la Windows. Pentru a utiliza această sarcină, trebuie să o programați să ruleze la pornirea sistemului. În mod implicit, scanarea autologon este dezactivată.

Sarcină implicită	Descriere
Documentele mele	Utilizați această sarcină pentru a scana directoare importante ale utilizatorului curent: `My Documents`, `Desktop` și `StartUp`. Astfel, veți asigura siguranța documentelor dumneavoastră, un spațiu de lucru sigur și rularea la pornirea sistemului a unor aplicații necompromise.

Dacă niciuna dintre aceste sarcini de scanare nu este potrivită scopului dumneavoastră, puteți crea o nouă sarcină de scanare, pe care o puteți programa apoi pentru a rula după cum este necesar.

4. Faceți clic-dreapta pe sarcina de scanare dorită și selectați **Planifică**. Va apărea o nouă fereastră.
5. Programați sarcina să ruleze după cum este necesar:
   - Pentru a rula sarcina de scanare o singură dată, selectați **O singură dată** și specificați data și ora începerii.
   - Pentru a rula sarcina de scanare la pornirea sistemului, selectați **La pornirea sistemului**. Puteți indica după cât timp de la pornirea sistemului să fie rulată sarcina (în minute).
   - Pentru a rula sarcina de scanare periodic, selectați **Periodic** și specificați cât de des să ruleze, precum și data și ora începerii.

   Notă

   De exemplu, pentru a vă scana calculatorul în fiecare sâmbătă, la ora 2 dimineața, trebuie să configurați programul după cum urmează:

   a. Selectați **Periodic**.

   b. În câmpul **La fiecare**, tastați 1 și apoi selectați **săptămâni** din meniu. În acest fel, sarcina este rulată o dată pe săptămână.

   c. Setați ca dată de început următoarea zi de sâmbătă.

   d. Setați ora începerii la `2:00:00` .

6. Faceți clic pe **OK** pentru a salva programul. Sarcina de scanare va rula în mod automat conform programului pe care l-ați definit. Dacă aveți calculatorul închis atunci când sarcina trebuie să ruleze, aceasta va fi executată imediat ce deschideți calculatorul.

Remedierea problemelor și asistența

35. Remedierea problemelor

Acest capitol prezintă unele probleme care pot apărea atunci când folosiți BitDefender și vă oferă soluții posibile. Majoritatea acestor probleme pot fi remediate prin configurarea adecvată a setărilor de produs.

Dacă problema dvs nu este prezentată aici sau dacă soluțiile oferite nu vă sunt de ajutor, puteți contacta echipa de suport tehnic BitDefender folosind informațiile din capitolul *„Suport”* (p. 332).

35.1. Probleme la instalare

Acest articol vă ajută să remediați problemele care apar cel mai des la instalarea BitDefender. Aceste probleme pot face parte din următoarele categorii:

- Erori de validare a instalării: asistentul de instalare nu pot fi rulat din cauza unei anumite situații a sistemului dvs.
- Instalări eșuate: ați inițiat instalarea din asistentul de instalare, dar procesul nu s-a finalizat.

35.1.1. Erori de validare a instalării

Când porniți asistentul de instalare, sunt verificate o serie de condiții pentru validarea necesară inițierii instalării. În tabelul de mai jos sunt prezentate cel mai des întâlnite erori de validare a instalării și soluțiile pentru remedierea lor.

Eroare	Descriere & Soluție
Nu aveți drepturile necesare pentru instalarea programului.	Pentru a rula asistentul de instalare și pentru a instala BitDefender, aveți nevoie de drepturi de administrator. Puteți proceda în oricare dintre următoarele modalități: ● Conectați-vă la un cont Windows de administrator și rulați din nou asistentul de instalare. ● Faceți clic-dreapta pe fișierul de instalare și selectați **Rulează ca**. Introduceți numele de utilizator și parola corespunzătoare unui cont Windows de administrator al sistemului.
Programul de instalare a detectat o versiune anterioară BitDefender, care nu a fost dezinstalată corect.	BitDefender a fost instalat anterior pe sistemul dvs, dar versiunea respectivă nu a fost dezinstalată complet. Acest fapt împiedică instalarea unei noi versiuni BitDefender. Pentru a remedia această eroare și pentru a instala BitDefender, urmați acești pași:

Eroare	Descriere & Soluție
	1. Mergeți la www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dvs. 2. Rulați instrumentul de dezinstalare folosind drepturile de administrare a sistemului. 3. Reporniți calculatorul. 4. Reporniți asistentul de instalare BitDefender.
Produsul BitDefender nu este compatibil cu sistemul dvs de operare.	Încercați să instalați BitDefender pe un sistem de operare cu care acesta nu este compatibil. Consultați *„Cerințe de sistem"* (p. 2) pentru a afla care sunt sistemele de operare care permit instalarea BitDefender. Dacă sistemul dvs de operare este Windows XP cu Service Pack 1 sau fără nici un pachet de servicii, puteți să instalați Service Pack 2 sau mai recent și apoi să rulați din nou asistentul de instalare.
Fișierul de instalare este proiectat pentru un alt tip de procesor.	Dacă obțineți o astfel de eroare, înseamnă că încercați să rulați o versiune incorectă a fișierului de instalare. Există două versiuni ale fișierului de instalare BitDefender: una pentru procesoare pe 32 de biți și cealaltă pentru procesoare pe 64 de biți. Pentru a vă asigura că aveți versiunea corectă pentru sistemul dvs, descărcați fișierul de instalare direct de la www.bitdefender.com .

35.1.2. Instalare eșuată

Există mai multe cauze posibile ale unei instalări eșuate:

- În timpul instalării apare un ecran de eroare. Vi se poate solicita să anulați instalarea sau vi se poate pune la dispoziție un buton prin care să rulați un instrument de dezinstalare, care va curăța sistemul.

  Notă
  Imediat după inițierea instalării BitDefender, puteți fi informat că nu există suficient spațiu liber pe disc. În acest caz, eliberați spațiul necesar pe partiția pe care doriți să instalați BitDefender și apoi reluați sau reinițiati instalarea.

- Instalarea nu înaintează și, eventual, sistemul se blochează. Sistemul reacționează numai după repornire.

- Instalarea s-a finalizat, dar nu puteți folosi funcțiile BitDefender, parțial sau în totalitate.

Pentru a reuși instalarea BitDefender după o tentativă eșuată, urmați acești pași:

1. **Curățați sistemul după instalarea eșuată.** Dacă instalarea eșuează, unele chei de regiștri și fișiere BitDefender por rămâne în sistemul dvs. Aceste rămășite pot împiedica instalarea ulterioară a BitDefender. De asemenea, ele pot afecta funcționarea și stabilitatea sistemului. De aceea, este necesar să le ștergeți înainte de a încerca să reinstalați produsul.

   Dacă pe ecranul de eroare apare un buton de rulare a unui instrument de dezinstalare, faceți clic pe el pentru a curăța sistemul. În caz contrar, procedați după cum urmează:

   a. Mergeți la www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dvs.

   b. Rulați instrumentul de dezinstalare folosind drepturile de administrare a sistemului.

   c. Reporniți calculatorul.

2. **Verificați cauzele posibile ale instalării eșuate.** Înainte de a începe reinstalarea produsului, verificați dacă există și eliminați posibilele cauze ale instalării inițiale eșuate:

   a. Verificați dacă aveți instalată orice altă soluție de securitate pentru că ea ar putea perturba funcționarea normală a BitDefender. Vă recomandăm să dezinstalați toate celelalte soluții de securitate și apoi să reinstalați BitDefender.

   b. De asemenea, este recomandat să verificați dacă sistemul dvs este infectat. Puteți proceda în oricare dintre următoarele modalități:

      - Folosiți CD-ul BitDefender de repornire în situații de urgență (rescue CD) și eliminați orice pericol existent. Pentru mai multe informații, consultați capitolul „BitDefender Rescue CD” (p. 335).

      - Deschideți o fereastra Internet Explorer, mergeți la www.bitdefender.com și efectuați o scanare online (faceți clic pe butonul **Scanare online**).

3. Încercați din nou să instalați BitDefender. Este recomandat să descărcați și să rulați cea mai recentă versiune a fișierului de instalare de pe www.bitdefender.ro.

4. Dacă instalarea eșuează, vă rugăm să contactați BitDefender pentru suport, folosind informațiile din secțiunea „*Suport*” (p. 332).

35.2. Serviciile BitDefender nu răspund

Acest articol vă ajută să remediați problema *Serviciile BitDefender nu răspund*. Această problemă poate apărea în următoarele situații:

- Iconița BitDefender din bara de sistem apare în gri și o fereastră pop-up vă informează că serviciile BitDefender nu răspund.
- Fereastra BitDefender indică faptul că serviciile BitDefender nu răspund.

Problema poate fi cauzată de:

- o actualizare importantă este în curs de instalare.
- erori temporare de comunicare între serviciile BitDefender.
- unele dintre serviciile BitDefender sunt oprite.
- alte soluții de securitate rulează pe calculatorul dvs, în același timp cu BitDefender.
- viruși de pe sistemul dvs afectează funcționarea normală a BitDefender.

Pentru a remedia această problemă, încercați următoarele soluții:

1. Așteptați câteva momente pentru a vedea dacă apar schimbări. Eroarea poate fi temporară.
2. Reporniți calculatorul și așteptați câteva momente până când se încarcă BitDefender. Deschideți BitDefender pentru a vedea dacă eroarea persistă. De obicei, repornirea calculatorului rezolvă problema.
3. Verificați dacă aveți instalată orice altă soluție de securitate pentru că ea ar putea perturba funcționarea normală a BitDefender. Vă recomandăm să dezinstalați toate celelalte soluții de securitate și apoi să reinstalați BitDefender.
4. Dacă eroarea persistă, este posibil să existe o problemă mai gravă (de exemplu, calculatorul dvs ar putea fi infectat cu un virus care afectează funcționarea BitDefender). Vă rugăm să contactați BitDefender pentru suport, folosind informațiile din secțiunea *„Suport”* (p. 332).

35.3. Nu se pot partaja fișiere și imprimante în rețeaua Wi-Fi (Wireless)

Acest articol vă ajută să remediați următoarele probleme care pot afecta Firewallul BitDefender în rețelele Wi-Fi:

- Calculatoarele din rețeaua Wi-Fi nu pot accesa fișierele partajate.
- Nu se poate accesa o imprimantă de rețea atașată la rețeaua Wi-Fi.
- Nu se poate accesa imprimanta partajată de un calculator din rețeaua Wi-Fi.
- Nu puteți partaja imprimanta dvs cu calculatoare din rețeaua Wi-Fi.

Înainte de a începe remedierea acestor probleme, este necesar să cunoașteți câteva lucruri despre securitate și configurarea firewallului BitDefender în rețelele Wi-Fi. Din punctul de vedere al securității, rețelele Wi-Fi se încadrează în una dintre aceste categorii:

- **Rețele Wi-Fi securizate.** Acest tip de rețea permite numai conectarea dispozitivelor autorizate, care au funcția Wi-Fi activată. Accesul la rețea este condiționat de furnizarea unei parole. Un exemplu de rețelele Wi-Fi securizate este cel al rețelelor de birou.
- **Rețele Wi-Fi deschise (nesecurizate).** Orice dispozitiv pe care a fost activată funcția Wi-Fi și care se află în aria de acoperire a unei rețele Wi-Fi nesecurizate poate să se conecteze la aceasta. Rețelele Wi-Fi nesecurizate sunt folosite foarte des. În această categorie intră aproape orice rețea Wi-Fi publică (cum ar fi cele din campusuri școlare, cafenele, aeroporturi și altele). Rețeaua personală pe care o creați cu ajutorul unui router wireless, este, de asemenea, nesecurizată până când nu activați opțiunile de securitate ale router-ului.

  Rețelele Wi-Fi nesecurizate prezintă un mare risc, deoarece calculatorul dvs este conectat la calculatoare necunoscute. Fără protecția adecvată furnizată de un firewall, oricine se conectează la rețea poate accesa fișierele dvs partajate și poate chiar pătrunde în mod fraudulos în calculatorul dvs.

În momentul conectării la o rețea Wi-Fi nesecurizată, BitDefender blochează automat comunicarea cu calculatoarele din acea rețea. Aveți acces numai la Internet, dar nu puteți partaja fișiere sau imprimante cu alți utilizatori din rețea.

Pentru a permite comunicarea cu o rețea Wi-Fi, există două soluții:

- Soluția "calculatoare sigure" permite partajarea de fișiere și imprimante numai cu anumite calculatoare (calculatoare sigure) din rețeaua Wi-Fi. Folosiți această soluție, atunci când sunteți conectat la o rețea Wi-Fi publică (de exemplu într-un campus sau într-o cafenea) și doriți să partajați fișiere sau o imprimantă cu un prieten sau să accesați o imprimantă din rețeaua Wi-Fi.
- Soluția "rețea sigură" permite partajarea de fișiere și imprimante în întreaga rețea Wi-Fi (rețea sigură). Această soluție nu este recomandată, din motive de securitate, dar poate fi utilă în anumite situații (de exemplu, pentru rețeaua Wi-Fi de acasă sau de la birou).

35.3.1. Soluția "Calculatoare sigure"

Pentru a configura firwallul BitDefender să permite partajarea de fișiere și imprimante cu un calculator din rețea Wi-Fi sau accesul la o imprimantă din rețeaua Wi-Fi, urmați acești pași:

1. Deschideți BitDefender și treceți interfața în Modul Expert.
2. Faceți clic pe **Firewall** în meniul din stânga.
3. Faceți clic pe tabul **Rețeai**.
4. În tabelul Zone, selectați rețeaua Wi-Fi și apoi faceți clic pe butonul **Adaugă**.

5. Selectați calculatorul sau imprimanta dorit/ă din lista de unități detectate în rețeaua Wi-Fi. Dacă calculatorul sau imprimanta în cauză nu au fost detectate în mod automat, puteți introduce adresa lor IP în câmpul **Zonă**.
6. Selectați acțiunea **Permite**.
7. Faceți clic pe **OK**.

Dacă tot nu puteți să partajați fișiere sau o imprimantă cu calculatorul selectat, este foarte probabil ca acest lucru să nu se datoreze firewallului BitDefender de pe calculatorul dvs. Verificați alte cauze posibile, cum ar fi:

- Firewallul de pe celălalt calculator poate bloca partajarea de fișiere și imprimante în rețelele Wi-Fi nesigure (publice).
  - Dacă firewallul este cel al unui produs BitDefender 2009 sau 2010, trebuie urmată aceeași procedură pe celălalt calculator pentru a se permite partajarea de fișiere și imprimante cu calculatorul dvs.
  - Dacă se folosește Windows Firewall, acesta poate fi configurat să permită partajarea de fișiere, după cum urmează: deschideți fereastra de setări a Windows Firewall, tabul **Excepții**, și selectați căsuța **Partajare fișiere și imprimante**.
  - Dacă se folsește un alt program firewall, consultați documentația sau fișierul de ajutor ale acestuia.
- Cauze generale care pot împiedica folosirea sau conectarea la imprimanta partajată:
  - Poate fi necesar să vă conectați la un cont Windows de administrator pentru a avea acces la imprimanta partajată.
  - Numai anumite calculatoare și anumiți utilizatori pot accesa imprimanta partajată. Dacă partajați imprimanta dvs, verificați restricțiile de acces stabilite pentru aceasta pentru a vedea dacă utilizatorul de pe celălalt calculator o poate accesa. Dacă încercați să vă conectați la o imprimantă partajată, întrebați utilizatorul de pe celălalt calculator dacă vi se permite accesul la imprimantă.
  - Imprimanta conectată la calculatorul dvs sau la celălalt calculator nu este partajată.
  - Imprimanta partajată nu este adăugată pe calculator.

Notă

Pentru a afla cum să administrați imprimantele partajate (partajare, stabilirea sau eliminarea permisiunii de acces la o imprimantă, conectarea la o imprimantă de rețea sau partajată), mergeți la Centrul de Asistență și Suport Windows (în meniul Start, faceți clic pe **Asistență și suport**).

Dacă tot nu puteți să accesați imprimanta din rețeaua Wi-Fi, este foarte probabil ca acest lucru să nu se datoreze firewallului BitDefender de pe calculatorul dvs. Accesul la imprimanta din rețeaua Wi-Fi poate fi restricționat pentru anumite calculatoare sau pentru anumiți utilizatori. Este recomandat să consultați administratorul rețelei Wi-Fi pentru a afla dacă vă puteți conecta la imprimanta în cauză.

Dacă bănuiți că problema se datorează firewallului BitDefender, puteți contacta BitDefender pentru suport, folosind informațiile din secțiunea *„Suport”* (p. 332).

35.3.2. Soluția "Rețea sigură"

Se recomandă să nu folosiți această soluție decât pentru rețelele Wi-Fi de acasă sau de la birou.

Pentru a configura firewallul BitDefender să permită partajarea de fișiere și imprimante cu întreaga rețea Wi-Fi, urmați acești pași:

1. Deschideți BitDefender și treceți interfața în Modul Expert.
2. Faceți clic pe **Firewall** în meniul din stânga.
3. Faceți clic pe tabul **Rețeai**.
4. În tabelul Configurare rețea, coloana **Nivel încredere**, faceți clic pe săgeata din celula corespunzătoare rețelei Wi-Fi.
5. În funcție de nivelul de securitate pe care doriți să-l obțineți, alegeți una dintre următoarele opțiuni:
   - **Nesigur** - pentru a accesa fișierele și imprimantele partajate în rețeaua Wi-Fi, fără a permite accesul la fișierele dvs partajate.
   - **Sigur** - pentru a permite partajarea de fișiere și imprimante în ambele sensuri. Astfel, utilizatorii conectați la rețeaua Wi-Fi pot accesa și fișierele sau imprimanta partajate de dvs.

Dacă tot nu puteți să partajați fișiere sau o imprimantă cu anumite calculatoare din rețeaua Wi-Fi, este foarte probabil ca acest lucru să nu se datoreze firewallului BitDefender de pe calculatorul dvs. Verificați alte cauze posibile, cum ar fi:

- Firewallul de pe celălalt calculator poate bloca partajarea de fișiere și imprimante în rețelele Wi-Fi nesigure (publice).
  - Dacă firewallul este cel al unui produs BitDefender 2009 sau 2010, trebuie urmată aceeași procedură pe celălalt calculator pentru a se permite partajarea de fișiere și imprimante cu calculatorul dvs.
  - Dacă se folosește Windows Firewall, acesta poate fi configurat să permită partajarea de fișiere, după cum urmează: deschideți fereastra de setări a Windows Firewall, tabul **Excepții**, și selectați căsuța **Partajare fișiere și imprimante**.

- Dacă se folsește un alt program firewall, consultați documentația sau fișierul de ajutor ale acestuia.

- Cauze generale care pot împiedica folosirea sau conectarea la imprimanta partajată:
  - Poate fi necesar să vă conectați la un cont Windows de administrator pentru a avea acces la imprimanta partajată.
  - Numai anumite calculatoare și anumiți utilizatori pot accesa imprimanta partajată. Dacă partajați imprimanta dvs, verificați restricțiile de acces stabilite pentru aceasta pentru a vedea dacă utilizatorul de pe celălalt calculator o poate accesa. Dacă încercați să vă conectați la o imprimantă partajată, întrebați utilizatorul de pe celălalt calculator dacă vi se permite accesul la imprimantă.
  - Imprimanta conectată la calculatorul dvs sau la celălalt calculator nu este partajată.
  - Imprimanta partajată nu este adăugată pe calculator.

Notă

Pentru a afla cum să administrați imprimantele partajate (partajare, stabilirea sau eliminarea permisiunii de acces la o imprimantă, conectarea la o imprimantă de rețea sau partajată), mergeți la Centrul de Asistență și Suport Windows (în meniul Start, faceți clic pe **Asistență și suport**).

Dacă tot nu puteți să accesați o imprimantă din rețeaua Wi-Fi, este foarte probabil ca acest lucru să nu se datoreze firewallului BitDefender de pe calculatorul dvs. Accesul la imprimanta din rețeaua Wi-Fi poate fi restricționat pentru anumite calculatoare sau pentru anumiți utilizatori. Este recomandat să consultați administratorul rețelei Wi-Fi pentru a afla dacă vă puteți conecta la imprimanta în cauză.

Dacă bănuiți că problema se datorează firewallului BitDefender, puteți contacta BitDefender pentru suport, folosind informațiile din secțiunea *„Suport”* (p. 332).

35.4. Filtrul Antispam nu funcționează corect

Acest articol vă ajută să remediați următoarele probleme legate de funcționarea filtrului Antispam BitDefender:

- Mai multe mesaje e-mail legitime sunt marcate ca `[spam]`.
- Multe mesaje spam nu sunt marcate corespunzător de filtrul antispam.
- Filtrul antispam nu detectează niciun mesaj spam.

35.4.1. Mesaje legitime sunt marcate ca [spam]

Mesaje legitime sunt marcate ca `[spam]` pentru că filtrul antispam BitDefender le percepe ca atare. În mod normal, puteți rezolva această problemă printr-o configurare adecvată a filtrului Antispam.

BitDefender adaugă automat destinatarii mesajelor dvs e-mail pe o Listă de prieteni. Mesajele e-mail primite de la persoanele de pe Lista de prieteni sunt considerate a fi legitime. Ele nu sunt verificate de filtrul antispam și, astfel, nu sunt marcate niciodată ca `[spam]`.

Configurarea automată a Listei de prieteni nu previne erorile de detecție care pot apărea în următoarele situații:

- Primiți multe mesaje comerciale nesolicitate, ca urmare a înscrierii pe diferite site-uri web. În acest caz, soluția este să adăugați adresele de e-mail de la care primiți astfel de mesaje pe Lista de prieteni.
- O parte semnificativă a mesajelor e-mail pe care le primiți sunt trimise de oameni cărora nu le-ați scris niciodată pe e-mail, cum ar fi: clienți, potențiali parteneri de afaceri și alții. În acest caz, sunt necesare alte soluții.

Dacă folosiți unul dintre clienții de mail în care BitDefender se integrează, încercați următoarele soluții:

1. Indica erorile de detecție. Aceasta folosește la antrenarea Motorului de învățare (Bayesian) al filtrului antispam și permite prevenirea erorilor de detecție ulterioare. Motorul de învățare analizează mesajele indicate și învață tiparele acestora. Următoarele mesaje e-mail care corespund acelor tipare nu vor fi marcate ca `[spam]`.
2. Redu nivelului de protecție antispam. Prin scăderea nivelului de protecție antispam, filtru antispam va avea nevoie de mai multe indicii pentru a clasifica un mesaj e-mail ca spam. Încercați această soluție numai dacă multe mesaje legitime (inclusiv mesaje comerciale solicitate) sunt incorect detectate ca spam.
3. Reantrenează Motorul de învățare (filtrul Bayesian). Încercați această soluție numai dacă soluțiile anterioare nu au dat rezultate satisfăcătoare.

Notă

BitDefender se integrează în cel mai frecvent utilizați clienți de mail, printr-o bara de instrumente antispam ușor de utilizat. Pentru o listă completă a clienților de mail admiși, vă rugăm să accesați *„Aplicații în care se poate integra BitDefender ”* (p. 2).

Dacă folosiți un alt client de mail, nu puteți indica erorile de detecție și antrena Motorul de învățare. Pentru a rezolva problema, încercați să reduceți nivelului protecției antispam.

Adăugă contactele pe Lista de prieteni

Dacă folosiți un client de mail admis, puteți adăuga foarte ușor expeditorii de mesaje legitime pe Lista de prieteni. Urmați pașii:

1. În clientul dvs de mail, selectați un mesaj e-mail al expeditorului pe care doriți să-l adăugați pe Lista de prieteni.
2. Faceți clic pe butonul **Adaugă prieten** din bara de instrumente antispam BitDefender.
3. Vi se poate cere să confirmați adresa adăugată pe Lista de prieteni. Selectați **Nu mai afișa acest mesaj** și faceți clic pe **OK**.

Veți primi toate mesajele de la această adresă, indiferent de conținutul lor.

Dacă folosiți un alt client de mail, puteți adăuga contacte pe Lista de prieteni din interfața BitDefender. Urmați pașii:

1. Deschideți BitDefender și treceți interfața în Modul Expert.
2. Faceți clic pe **Antispam** în meniul din stânga.
3. Faceți clic pe tabul **Stare**.
4. Faceți clic pe **Administrează prieteni**. Va apărea o fereastră de configurare.
5. Introduceți adresa de e-mail a expeditorului de la care doriți să primiți întotdeauna mesaje e-mail și faceți clic pe butonul pentru a adăuga adresa pe Lista de prieteni.
6. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Indicați erorile de detecție

Dacă folosiți un client de mail admis, puteți corecta cu ușurință filtrul antispam (indicând care mesaje e-mail nu ar trebui marcate ca `[spam]`). Astfel, veți îmbunătăți considerabil eficiența filtrului antispam. Urmați pașii:

1. Deschideți clientul dvs de mail.
2. Mergeți în directorul cu mesaje nesolicitate (junk), în care sunt mutate mesajele spam.
3. Selectați mesajele legitime pe care BitDefender le-a marcat incorect ca `[spam]`.
4. Faceți clic pe butonul **Adaugă prieten** din bara de instrumente antispam BitDefender, pentru a adăuga expeditorul pe Lista de prieteni. Este posibil să vi se ceară să faceți clic pe **OK**, pentru confirmare. Veți primi toate mesajele de la această adresă, indiferent de conținutul lor.
5. Faceți clic pe butonul **Nu este Spam** din bara de instrumente antispam BitDefender (localizată, de obicei, în zona de sus a ferestrei clientului de mail). Aceasta îi indică Motorului de învățare faptul că mesajul selectat nu este spam.

Mesajul e-mail va fi mutat în directorul Primite. Următoarele mesaje e-mail care corespund acelor tipare nu vor mai fi marcate ca [spam].

Reduceți nivelul protecției antispam

Pentru a reduce nivelul protecției antispam, urmați acești pași:

1. Deschideți BitDefender și treceți interfața în Modul Expert.
2. Faceți clic pe **Antispam** în meniul din stânga.
3. Faceți clic pe tabul **Stare**.
4. Mutați cursorul mai jos pe scală.

Este recomandat să reduceți protecția numai cu un nivel și apoi să așteptați îndeajuns de mult timp încât să puteți evalua rezultatele. Dacă multe mesaje e-mail legitime sunt încă marcate ca [spam], puteți reduce și mai mult nivelul protecției antispam. Dacă observați că numeroase mesaje spam nu sunt detectate, este recomandat să nu reduceți nivelul protecției antispam.

Re-educați Motorul de învățare (Bayesian)

Înainte de a educa Motorul de învățare (Bayesian), pregătiți un director care să conțină numai mesaje SPAM și un altul doar cu mesaje legitime. Motorul de învățare le va analiza și va învăța caracteristicile definitorii pentru mesajele spam sau legitime pe care le primiți de obicei. Pentru ca educarea să fie eficientă, trebuie să existe cel puțin 50 de mesaje din fiecare categorie.

Pentru a reseta baza de date Bayesiana și pentru a re-educa Motorul de învățare, urmați acești pași:

1. Deschideți clientul dvs de mail.
2. Pe bara de instrumente antispam BitDefender, faceți clic pe butonul **Asistent** pentru a porni programul asistent de configurare antispam. Pentru informații detaliate despre acest asistent, vă rugăm să consultați secțiunea *„Asistentul de configurare Antispam”* (p. 292).
3. Faceți clic pe **Înainte**.
4. Selectați **Sari peste acest pas** și faceți clic pe **Înainte**.
5. Selectați **Șterge baza de date antispam** și faceți clic pe **Înainte**.
6. Selectați directorul care conține mesaje legitime și faceți clic pe **Înainte**.
7. Selectați directorul care conține mesaje SPAM și faceți clic pe **Înainte**.
8. Faceți clic pe **Finalizare** pentru a începe procesul de educare.
9. Când educarea a luat sfârșit, faceți clic pe **Închide**.

Solicitați ajutor

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru suport, conform descrierii din secțiunea *„Suport”* (p. 332).

35.4.2. Multe mesaje spam nu sunt detectate

Dacă primiți multe mesaje spam care nu sunt marcate [spam], trebuie să configurați filtrul antispam BitDefender, pentru a-i îmbunătăți eficiența.

Dacă folosiți unul dintre clienții de mail în care BitDefender se integrează, încercați următoarele soluții, pe rând:

1. Indicați erorile de detecție. Aceasta folosește la antrenarea Motorului de învățare (Bayesian) al filtrului antispam și, de obicei, îmbunătățește eficiența detecției antispam. Motorul de învățare analizează mesajele indicate și învață tiparele acestora. Următoarele mesaje e-mail care corespund acelor tipare vor fi marcate ca [spam].
2. Adăugați spammerii pe Lista de spammeri. Mesajele e-mail primite de la adrese de pe Lista de spammeri sunt marcate automat ca [spam].
3. Sporiți nivelul protecției antispam. Prin creșterea nivelului de protecție antispam, filtru antispam va avea nevoie de mai puține indicii pentru a clasifica un mesaj e-mail ca spam.
4. Re-educați Motorul de învățare (filtrul Bayesian). Folosiți această soluție când detecția antispam nu mai este eficientă și indicarea mesajelor spam nedetectate nu mai funcționează.

Notă

BitDefender se integrează în cel mai frecvent utilizați clienți de mail, printr-o bara de instrumente antispam ușor de utilizat. Pentru o listă completă a clienților de mail admiși, vă rugăm să accesați *„Aplicații în care se poate integra BitDefender ”* (p. 2).

Dacă folosiți un alt client de mail, nu puteți indica mesaje spam și antrena Motorul de învățare. Pentru a rezolva problema, încercați să măriți nivelului protecției antispam și să adăugați spammeri pe Lista de spammeri.

Indicați mesajele spam nedetectate

Dacă folosiți un client de mail admis, puteți indica cu ușurință care mesaje e-mail ar fi trebuit să fie detectate ca spam. Astfel, veți îmbunătăți considerabil eficiența filtrului antispam. Urmați pașii:

1. Deschideți clientul dvs de mail.
2. Mergeți la directorul Primite.
3. Selectați mesajele spam nedetectate.

4. Faceți clic pe butonul **Este Spam** din bara de instrumente antispam BitDefender (localizată, de obicei, în zona de sus a ferestrei clientului de mail). Aceasta îi indică Motorului de învățare faptul că mesajele selectate sunt spam. Acestea sunt marcate imediat ca `[spam]` și mutate în directorul de mesaje nesolicitate (junk). Următoarele mesaje e-mail care corespund acelor tipare vor fi marcate ca `[spam]`.

Adăugați spammeri pe Lista de spammeri

Dacă folosiți un client de mail admis, puteți adăuga foarte ușor expeditorii de mesaje spam pe Lista de spammeri. Urmați pașii:

1. Deschideți clientul dvs de mail.
2. Mergeți în directorul cu mesaje nesolicitate (junk), în care sunt mutate mesajele spam.
3. Selectați mesajele pe care BitDefender le-a marcat ca `[spam]`.
4. Faceți clic pe butonul **Adaugă spammer** din bara de instrumente antispam BitDefender.
5. Vi se poate cere să confirmați adresa adăugată pe Lista de spammeri. Selectați **Nu mai afișa acest mesaj** și faceți clic pe **OK**.

Dacă folosiți un alt client de mail, puteți să adăugați manual spammeri pe Lista de spammeri, din interfața BitDefender. Este recomandat să procedați astfel numai atunci când ați primit mai multe mesaje spam de la aceeași adresă de e-mail. Urmați pașii:

1. Deschideți BitDefender și treceți interfața în Modul Expert.
2. Faceți clic pe **Antispam** în meniul din stânga.
3. Faceți clic pe tabul **Stare**.
4. Faceți clic pe **Administrează spammeri**. Va apărea o fereastră de configurare.
5. Introduceți adresa de e-mail a spammerului și faceți clic pe butonul pentru a adăuga adresa pe Lista de spammeri.
6. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Sporiți nivelul protecției antispam

Pentru a crește nivelul protecției antispam, urmați acești pași:

1. Deschideți BitDefender și treceți interfața în Modul Expert.
2. Faceți clic pe **Antispam** în meniul din stânga.
3. Faceți clic pe tabul **Stare**.
4. Mutați cursorul mai sus pe scală.

Re-educați Motorul de învățare (Bayesian)

Înainte de a educa Motorul de învățare (Bayesian), pregătiți un director care să conțină numai mesaje SPAM și un altul doar cu mesaje legitime. Motorul de învățare le va analiza și va învăța caracteristicile definitorii pentru mesajele spam sau legitime pe care le primiți de obicei. Pentru ca educarea să fie eficientă, trebuie să existe cel puțin 50 de mesaje în fiecare categorie.

Pentru a reseta baza de date Bayesiana și pentru a re-educa Motorul de învățare, urmați acești pași:

1. Deschideți clientul dvs de mail.
2. Pe bara de instrumente antispam BitDefender, faceți clic pe butonul **Asistent** pentru a porni programul asistent de configurare antispam. Pentru informații detaliate despre acest asistent, vă rugăm să consultați secțiunea *„Asistentul de configurare Antispam"* (p. 292).
3. Faceți clic pe **Înainte**.
4. Selectați **Sari peste acest pas** și faceți clic pe **Înainte**.
5. Selectați **Șterge baza de date antispam** și faceți clic pe **Înainte**.
6. Selectați directorul care conține mesaje legitime și faceți clic pe **Înainte**.
7. Selectați directorul care conține mesaje SPAM și faceți clic pe **Înainte**.
8. Faceți clic pe **Finalizare** pentru a începe procesul de educare.
9. Când educarea a luat sfârșit, faceți clic pe **Închide**.

Solicitați ajutor

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru suport, conform descrierii din secțiunea *„Suport"* (p. 332).

35.4.3. Filtrul antispam nu detectează niciun mesaj spam

Dacă niciun mesaj spam nu este marcat ca `[spam]`, este posibil să existe probleme legate de filtrul Antispam BitDefender. Înainte de a remedia această problemă, asigurați-vă că ea nu se datorează următoarelor cauze:

- Protecția Antispam BitDefender este disponibilă numai pentru clienții de e-mail configurați să primească mesaje e-mail prin protocolul POP3. Aceasta înseamnă că:
  - Mesajele e-mail primite prin servicii de e-mail bazate pe web (cum ar fi Yahoo, Gmail, Hotmail sau altele) nu sunt filtrate antispam de BitDefender.
  - Dacă aveți un client de e-mail configurat să primească mesaje prin alt protocol decât POP3 (de exemplu IMAP4), filtrul BitDefender Antispam nu supune aceste mesaje unei verificări antispam.

Notă

POP3 este unul dintre cele mai des folosite protocoale de descărcare a mesajelor e-mail de pe un server de mail. Dacă nu știți ce protocol folosește clientul dvs de e-mail pentru a descărca mesajele, întrebați persoana care l-a configurat.

- BitDefender Internet Security 2010 nu scanează traficul POP3 generat de Lotus Notes.

Verificați, de asemenea, dacă nu a intervenit una din următoarele cauze:

1. Asigurați-vă că modulul Antispam este activat.
   a. Deschideți BitDefender.
   b. Faceți clic pe butonul **Setări** din colțul din dreapta, sus al ferestrei.
   c. În categoria Setări de securitate, verificați starea protecției antispam.

   Dacă protecția Antispam este dezactivată, aceasta este cauza problemei dvs. Activați protecția Antispam și monitorizați funcționarea acesteia pentru a vedea dacă problema este rezolvată.
2. Deși este puțin probabil, verificați dacă dvs (sau altcineva) ați configurat BitDefender să nu marcheze mesajele spam ca `[spam]`.
   a. Deschideți BitDefender și treceți interfața în Modul Expert.
   b. Faceți clic pe **Antispam** în meniul din stânga și apoi pe tabul **Setări**.
   c. Asigurați-vă că opțiunea **Marchează mesajele spam la subiect** este selectată.

O soluție posibilă este repararea sau reinstalarea produsului. Dacă doriți, puteți contacta BitDefender pentru suport, folosind informațiile din secțiunea *„Suport”* (p. 332).

35.5. Nu s-a reușit dezinstalarea BitDefender

Acest articol vă ajută să remediați erorile care pot apărea la dezinstalarea BitDefender. Sunt posibile două situații:

- În timpul dezinstalării apare un ecran de eroare. Ecranul oferă un buton pentru rularea unui instrument de dezinstalare, care va curăța sistemul.
- Dezinstalarea nu înaintează și, eventual, sistemul se blochează. Faceți clic pe **Anulare** pentru a abandona dezinstalarea. Dacă anularea nu este posibilă, reporniți sistemul.

Dacă dezinstalarea eșuează, unele chei de regiștri și fișiere BitDefender por rămâne în sistemul dvs. Aceste rămășite pot împiedica instalarea ulterioară a BitDefender. De asemenea, ele pot afecta funcționarea și stabilitatea sistemului. Pentru a dezinstala BitDefender complet de pe sistemul dvs, trebuie să rulați instrumentul de dezinstalare.

Dacă dezinstalarea nu reușește și se afișează un ecran de eroare, faceți clic pe butonul de rulare a instrumentul de dezinstalare, pentru a curăța sistemul. În caz contrar, procedați după cum urmează:

1. Mergeți la www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dvs.
2. Rulați instrumentul de dezinstalare folosind drepturile de administrare a sistemului. Utilitarul de dezinstalare va șterge toate fișierele și cheile din regiștri care nu au fost șterse în timpul procesului automatizat de dezinstalare.
3. Reporniți calculatorul.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru suport, conform descrierii din secțiunea „*Suport*” (p. 332).

36. Suport

BitDefender se străduiește să ofere clienților săi un nivel cât mai ridicat în ceea ce privește rapiditatea și calitatea suportului tehnic. BitDefender Knowledge Base (http://www.bitdefender.ro/suport) furnizează articole care conțin soluții la majoritatea problemelor și întrebărilor dumneavoastră legate de BitDefender. Dacă nu găsiți soluția în Knowledge Base, puteți contacta echipa de suport tehnic a BitDefender. Reprezentanții BitDefender vă vor răspunde la întrebări în timp util și vă vor oferi toată asistența de care aveți nevoie.

36.1. BitDefender Knowledge Base

BitDefender Knowledge Base este o bază online de informații despre produsele BitDefender. Stochează, într-un format accesibil, rapoarte ale echipelor de suport și dezvoltare cu privire la rezultatele suportului tehnic continuu și ale activităților de eliminare a bug-urilor BitDefender împreună cu articole mai generale despre prevenția virușilor, administrarea soluțiilor BitDefender și explicații detaliate, și multe alte articole.

BitDefender Knowledge Base este pusă la dispoziția publicului. Această multitudine de informații reprezintă încă o cale de a oferi clienților BitDefender asistența tehnică de care au nevoie. Toate cererile valide de informații sau rapoarte despre bug-uri venind de la clienții BitDefender ajung în cele din urmă în BitDefender Knowledge Base, ca rapoarte asupra eliminării bug-urilor, fișe de lucru sau articole informative pentru a suplimenta fișierele de suport ale produsului.

BitDefender Knowledge Base este disponibilă oricând la adresa http://kb.bitdefender.ro.

36.2. Solicitarea ajutorului

Puteți cere ajutor prin intermediul serviciului online de asistență al BitDefender. Urmați pașii de mai jos:

1. Mergeți la http://www.bitdefender.ro/suport. Aici se află BitDefender Knowledge Base. BitDefender Knowledge Base oferă numeroase articole care conțin soluții la probleme legate de utilizarea soluțiilor BitDefender.
2. Căutați în BitDefender Knowledge Base articole care vă pot ajuta să rezolvați problema pe care o întâmpinați.
3. Vă rugăm să citiți articolul relevant și să încercați soluția propusă.
4. Dacă soluția respectivă nu vă rezolvă problema, folosiți linkul din articol pentru a contacta echipa de suport tehnic a BitDefender.
5. Intrați în contul dumneavoastră BitDefender.
6. Contactați reprezentanții BiDefender prin e-mail, pe chat sau la telefon.

36.3. Informații de contact

Comunicarea eficientă este cheia unei afaceri de succes. În ultimii 10 ani BitDefender a câștigat o reputație indisputabilă în depășirea așteptărilor clienților și partenerilor, căutând în mod constant mijloace pentru o comunicare eficientă. Nu ezitați să ne contactați indiferent ce problemă sau întrebare ați avea.

36.3.1. Adrese Web

Departament de vânzări: sales@bitdefender.ro
Suport tehnic: kb.bitdefender.ro
Documentație: documentation@bitdefender.com
Programe de Parteneriat: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Relații Media: pr@bitdefender.com
Cariere: jobs@bitdefender.com
Subscrieri viruși: virus_submission@bitdefender.com
Subscrieri spam: spam_submission@bitdefender.com
Raportare abuz: abuse@bitdefender.com
Site produs: http://www.bitdefender.ro
Arhive ftp ale produsului: ftp://ftp.bitdefender.com/pub
Distribuitori locali: http://www.bitdefender.ro/site/Partnership/list/
BitDefender Knowledge Base: http://kb.bitdefender.ro

36.3.2. Filialele BitDefender

Sucursalele BitDefender sunt pregătite să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și pe cele generale. Adresele lor precum și modul în care pot fi contactate sunt date mai jos.

Romania

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax: +40 21 2641799
Telefon vânzări: +40 21 2063470
E-mail vânzări: sales@bitdefender.ro
Suport tehnic: http://www.bitdefender.ro/suport
Site web: http://www.bitdefender.ro

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309

Telefon (birou&vânzări): 1-954-776-6262
Vânzări: sales@bitdefender.com
Suport tehnic: http://www.bitdefender.com/help
Web: http://www.bitdefender.com

Germany

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Birou: +49 2301 91 84 222
Vânzări: vertrieb@bitdefender.de
Suport tehnic: http://kb.bitdefender.de
Web: http://www.bitdefender.de

Marea Britanie și Irlanda

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
E-mail: info@bitdefender.co.uk
Telefon: +44 (0) 8451-305096
Vânzări: sales@bitdefender.co.uk
Suport tehnic: http://www.bitdefender.com/help
Web: http://www.bitdefender.co.uk

Spain

BitDefender España SLU
C/ Balmes, 191, 2º, 1ª, 08006
Barcelona
Fax: +34 932179128
Telefon: +34 902190765
Vânzări: comercial@bitdefender.es
Suport tehnic: www.bitdefender.es/ayuda
Site web: http://www.bitdefender.es

BitDefender Rescue CD

37. Descriere generală

BitDefender Internet Security 2010 este furnizat cu un CD de boot (BitDefender Rescue CD) capabil a scana și dezinfecta tot calculatorul fără a fi necesară pornirea sistemului de operare.

Este indicat să utilizați BitDefender Rescue CD oricând sistemul dumneavoastră de operare nu funcționează corect din cauza infecției cu viruși. Aceasta se întâmplă în general când nu folosiți un produs antivirus.

Actualizarea definițiilor de viruși se face automat, fără intervenția utilizatorului de fiecare dată când este pornit BitDefender Rescue CD.

BitDefender Rescue CD este o distribuție Knoppix adaptată de BitDefender, care integrează cea mai recentă soluție de securitate BitDefender pentru Linux într-un CD GNU/Linux Knoppix Live, oferind un antivirus pentru desktop care este capabil să scaneze și să dezinfecteze hard discurile existente (incluzând partițiile Windows NTFS). De asemenea, BitDefender Rescue CD poate fi utilizat pentru a restaura datele dumneavoastră importante atunci când nu puteți porni Windowsul.

Notă

BitDefender Rescue CD poate fi descărcat de la această locație: http://download.bitdefender.com/rescue_cd/

37.1. Cerințe de sistem

Înainte de a porni BitDefender Rescue CD, trebuie să vă asigurați că sistemul dumneavoastră îndeplinește următoarele cerințe.

Tip procesor

Procesor compatibil cu x86, minimum 166 MHz, dar nu așteptați performanțe ridicate în acest caz. Un procesor de generație i686, la 800MHz, constituie o alegere mai bună.

Memorie

Minimum 512 MB memorie RAM (1 GB recomandat)

CD-ROM

BitDefender Rescue CD rulează de pe un CD-ROM, de aceea sunt necesare un CD-ROM și un BIOS capabil să-l pornească.

Conexiune Internet

Deși BitDefender Rescue CD va rula fără conexiune Internet, procedurile de actualizare vor necesita un link HTTP activ, chiar și printr-un server proxy. De aceea, pentru o protecție actualizată, conexiunea Internet este o CERINȚĂ.

Rezoluție grafică

Placă video standard compatibilă SVGA.

37.2. Soft inclus

BitDefender Rescue CD include următoarele pachete soft.

Xedit
Acesta este un editor text de fișiere.

Vim
Acesta este un editor text de fișiere avansat, oferind evidențierea sintaxei, o interfață grafică și multe altele. Pentru mai multe informații, consultați pagina web a Vim.

Xcalc
Acesta este un calculator.

RoxFiler
RoxFiler este manager de fișiere grafic, rapid și avansat.

Pentru mai multe informații, consultați pagina web a RoxFiler.

MidnightCommander
GNU Midnight Commander (mc) este un manager de fișiere în mod text.

Pentru mai multe informații, consultați pagina web a MC.

Pstree
Pstree afișează procesele care rulează.

Top
Top afișează sarcinile Linux.

Xkill
Xkill oprește un program care rulează în X.

Partition Image
Partition Image vă ajută să salvați partiții în format EXT2, Reiserfs, NTFS, HPFS, FAT16 și FAT32 într-un fișier imagine. Acest program poate fi util în scopuri de backup.

Pentru mai multe informații, consultați pagina web a Partimage.

GtkRecover
GtkRecover este o versiune GTK a programului de recuperare de consolă. Vă ajută să recuperați un fișier.

Pentru mai multe informații, consultați pagina web a GtkRecover.

ChkRootKit
ChkRootKit este un utilitar care vă ajută să vă scanați calculatorul după rootkituri.

Pentru mai multe informații, consultați pagina web a ChkRootKit.

Nessus Network Scanner

Nessus este un scaner de securitate remote pentru Linux, Solaris, FreeBSD și Mac OS X.

Pentru mai multe informații, consultați pagina web a Nessus.

Iptraf

Iptraf este un soft de monitorizare de rețea.

Pentru mai multe informații, consultați pagina web a Iptraf.

Iftop

Iftop afișează consumul de lățime de bandă pe o interfață.

Pentru mai multe informații, consultați pagina web a Iftop.

MTR

MTR este un utilitar de analiză de rețea.

Pentru mai multe informații, consultați pagina web a MTR.

PPPStatus

PPPStatus afișează statistici referitoare la traficul TCP/IP la intrare și la ieșire.

Pentru mai multe informații, consultați pagina web a PPPStatus.

Wavemon

Wavemon este o aplicație de monitorizare a dispozitivelor de rețea wireless.

Pentru mai multe informații, consultați pagina web a Wavemon.

USBView

USBView afișează informații despre dispozitivele conectate la magistrala USB.

Pentru mai multe informații, consultați pagina web a USBView.

Pppconfig

Pppconfig vă ajută să configurați automat o conexiune ppp prin dial-up.

DSL/PPPoe

DSL/PPPoe configurează o conexiune PPPoE (ADSL).

I810rotate

I810rotate activează ieșirea video pe hardware i810 utilizând i810switch(1).

Pentru mai multe informații, consultați pagina web a I810rotate.

Mutt

Mutt este un client de mail MIME avansat, cu interfață text.

Pentru mai multe informații, consultați pagina web a Mutt.

Mozilla Firefox

Mozilla Firefox este un browser web foarte popular.

Pentru mai multe informații, consultați pagina web a Mozilla Firefox.

Elinks

Elinks un browser web în mod text.

Pentru mai multe informații, consultați pagina web a Elinks.

38. Instrucțiuni BitDefender Rescue CD

Acest capitol conține informații despre pornirea și oprirea BitDefender Rescue CD, scanarea calculatorului dumneavoastră după aplicații malițioase precum și salvarea datelor de pe un PC cu Windows compromis pe un dispozitiv mobil. Totuși, utilizând aplicațiile software care sunt oferite pe CD, puteți executa numeroase alte sarcini, descrierea acestora fiind departe de scopul acestui manual de utilizare.

38.1. Pornirea BitDefender Rescue CD

Pentru a porni cd-ul, setați BIOS-ul calculatorului dumneavoastră să demareze de pe cd, așezați cd-ul în drive și reporniți calculatorul. Asigurați-vă că poate fi pornit calculatorul dumneavoastră de pe cd.

Așteptați până apare următorul ecran și urmați instrucțiunile pentru a porni BitDefender Rescue CD.

Ecran la pornirea sistemului

La pornirea sistemului, se face automat actualizarea semnăturilor de viruși. Procesul poate lua ceva timp.

La finalizarea procesului de pornire veți vedea următorul desktop. Acum puteți începe să utilizați BitDefender Rescue CD.

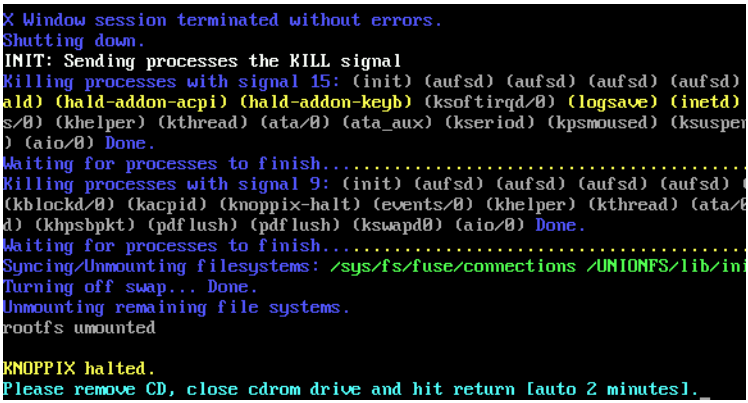
Desktopul

38.2. Oprirea BitDefender Rescue CD

Puteți închide calculatorul fără griji selectând **Închide** din meniul contextual BitDefender Rescue CD (faceți clic-dreapta pentru a-l deschide) sau introducând comanda **halt** într-un terminal.

Alegeți "EXIT"

Atunci când BitDefender Rescue CD a terminat de închis cu succes toate problemele va apărea un ecran ca cel din imagine. Puteți scoate cd-ul pentru a porni sistemul direct de pe hard drive. Acum puteți opri sau reporni calculatorul.



Așteptați acest mesaj înainte de oprire

38.3. Cum realizez o scanare antivirus?

După ce sistemul a fost pornit, va apărea un program asistent care vă permite să vă scanați complet calculatorul. Trebuie doar să faceți clic pe butonul **Start**.

Notă
Dacă rezoluția ecranului nu este suficient de mare, vi se va cere să porniți scanarea în mod text.

Urmați programul asistent în trei pași pentru a realiza procesul de scanare.

1. Puteți vedea stadiul și statisticile scanării (viteza de scanare, timpul scurs de la începutul scanării, numărul obiectelor scanate / infectate / suspecte / ascunse și altele).

   Notă
   Procesul de scanare poate dura destul de mult, în funcție de complexitatea scanării.

2. Puteți vedea numărul problemelor care vă afectează sistemul.

   Problemele sunt afișate pe grupuri. Faceți clic pe căsuța cu “+” pentru a deschide un grup sau pe căsuța cu “-” pentru a închide un grup.

   Puteți alege o acțiune globală care să fie luată asupra fiecărui grup de probleme sau puteți alege acțiuni separate pentru fiecare problemă în parte.
3. Puteți vedea un rezumat al rezultatelor.

Dacă doriți să scanați numai un anumit director, puteți folosi una dintre următoarele variante:

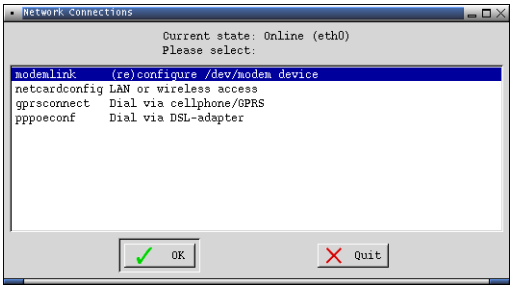
- Folosiți **BitDefender Scanner for Unices**.
  1. Faceți dublu-clic pe iconița START SCANNER de pe desktop. Aceasta va lansa **BitDefender Scanner for Unices**.
  2. Faceți clic pe **Scanner**. Va apărea o nouă fereastră.
  3. Selectați directorul pe care doriți să-l scanați și faceți clic pe **Open** pentru a începe scanarea folosind același asistent care a apărut atunci când ați pornit calculatorul prima dată.
- Folosiți meniul contextual - navigați printre fișiere, faceți clic-dreapta pe fișierul sau pe directorul dorit și selectați **Send to**. Apoi alegeți **BitDefender Scanner**.
- Sau puteți inițializa următoarea comandă de la un terminal. **BitDefender Antivirus Scanner** va începe cu fișierul sau directorul selectat ca locație implicită de scanare.

```
# bdscan /path/to/scan/
```

38.4. Cum configurez conexiunea Internet?

Dacă sunteți într-o rețea DHCP și aveți un card de rețea ethernet, conexiunea Internet ar trebui să fie deja detectată și configurată. Pentru configurare manuală, urmați pașii de mai jos.

1. Faceți dublu-clic pe iconița Network Connections (Conexiuni rețea) de pe desktop. Va apărea următoarea fereastră:



Network Connections (Conexiuni rețea)

2. Selectați tipul conexiunii utilizate și faceți clic pe OK.

Conexiune	Descriere
modemlink	Selectați acest tip de conexiune dacă folosiți un modem și o linie telefonică pentru acces la Internet.

Conexiune	Descriere
netcardconfig	Selectați acest tip de conexiune dacă folosiți o rețea locală (LAN) pentru acces la Internet. A se folosi și pentru conexiuni fără fir (wireless).
gprsconnect	Selectați acest tip de conexiune dacă accesați Internetul prin intermediul unei rețele de telefonie mobilă utilizând protocolul GPRS (General Packet Radio Service). Se poate folosi de asemenea un modem GPRS în locul unui telefon.
pppoeconf	Selectați acest tip de conexiune dacă folosiți un modem DSL (Digital Subscriber Line) pentru acces la Internet.

3. Urmați instrucțiunile de pe ecran. Dacă nu știți ce să scrieți, contactați administratorul sistemului sau rețelei dumneavoastră pentru detalii.

Important
Vă rugăm să țineți cont că prin selectarea opțiunilor de mai sus doar veți activa modemul. Pentru a configura conexiunea de rețea, urmați acești pași:

1. Faceți clic-dreapta pe desktop. Va apărea meniul contextual al BitDefender Rescue CD.
2. Selectați **Terminal (as root)**.
3. Introduceți următoarele comenzi:

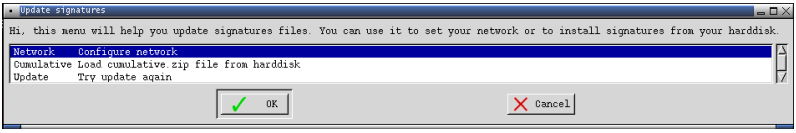
```
# pppconfig
```

4. Urmați instrucțiunile de pe ecran. Dacă nu știți ce să scrieți, contactați administratorul sistemului sau rețelei dumneavoastră pentru detalii.

38.5. Cum actualizez BitDefender?

La pornirea sistemului, actualizarea semnăturilor de viruși se face automat.Totuși, dacă ați sărit acest pas sau dacă doriți să actualizați BitDefender după pornirea calculatorului, iată două moduri în care puteți face acest lucru:

- Folosiți **BitDefender Scanner for Unices**.
  1. Faceți dublu-clic pe iconița START SCANNER de pe desktop. Aceasta va lansa **BitDefender Scanner for Unices**.
  2. Faceți clic pe **Actualizare**.
- Folosiți comanda rapidă **Update Signatures** de pe desktop.
  1. Faceți dublu-clic pe iconița Update Signatures de pe desktop. Va apărea următoarea fereastră:



Actualizare semnături

2. Puteți proceda astfel:
   - Selectați **Cumulative** pentru a instala semnăturile deja salvate pe hard discul dumneavoastră, căutând și încărcând fișierul `cumulative.zip`.
   - Selectați **Update** pentru a vă conecta imediat la internet și descărca ultimele semnături de viruși.
3. Faceți clic pe **OK**.

38.5.1. Cum actualizez BitDefender printr-un proxy?

Dacă folosiți un server proxy pentru conectarea calculatorului dumneavoastră la Internet, trebuie efectuate anumite configurări pentru a actualiza semnăturile de viruși.

Pentru a actualiza BitDefender printr-un proxy, folosiți una dintre următoarele opțiuni:

- Folosiți **BitDefender Scanner for Unices**.
  1. Faceți dublu-clic pe iconița START SCANNER de pe desktop. Aceasta va lansa **BitDefender Scanner for Unices**.
  2. Faceți clic pe **Settings**. Va apărea o nouă fereastră.
  3. Sub **Update Settings**, selectați căsuța **Enable HTTP Proxy**. Specificați gazda Proxy (a se preciza după cum urmează: `gazdă[:port]`), utilizatorul Proxy (a se preciza după cum urmează: `[domeniu\]utilizator`) și Parola. Selectați căsuța **Ocolire server proxy când nu este disponibil** pentru folosirea unei conexiuni directe dacă serverul proxy nu este disponibil.
  4. Faceți clic pe **Salvează**
  5. Faceți clic pe **Actualizează**
- Folosește Terminalul (ca root).
  1. Faceți clic-dreapta pe desktop. Va apărea meniul contextual al BitDefender Rescue CD.
  2. Selectați **Terminal (as root)**.
  3. Introduceți comanda: **cd /ramdisk/BitDefender-scanner/etc**.
  4. Introduceți comanda: **mcedit bdscan.conf** pentru a edita acest fișier utilizând GNU Midnight Commander (mc).
  5. Activați următoarea linie: `#HttpProxy =` (prin ștergerea simbolului #) și specificați domeniul, numele de utilizator, parola și portul serverului proxy. De exemplu, linia respectivă poate arăta astfel:

```
HttpProxy = myuser:mypassword@proxy.company.com:8080
```

6. Apăsați **F2** pentru a salva fișierul curent, confirmați salvarea și apoi apăsați **F10** pentru a-l închide.
7. Introduceți comanda: **bdscan update**.

38.6. Cum îmi salvez datele?

Să presupunem că nu puteți porni calculatorul dumneavoastră, cu Windows instalat, din cauza unor probleme necunoscute. În același timp, trebuie neapărat să accesați date importante de pe calculatorul dumneavoastră. Aici este util BitDefender Rescue CD.

Pentru a salva datele dumneavoastră de pe calculator pe un dispozitiv mobil, cum ar fi un stick de memorie USB, urmați acești pași:

1. Introduceți CD-ul cu BitDefender Rescue CD în unitatea CD-ROM, stickul de memorie în USB și apoi reporniți calculatorul.

   Notă

   Dacă introduceți stickul de memorie mai târziu, va trebui să montați dispozitivul amovibil urmând acești pași:

   a. Faceți dublu-clic pe iconița Terminal Emulator de pe desktop.

   b. Introduceți următoarea comandă:

   ```
   # mount  /media/sdb1
   ```

   Vă rugăm să țineți cont că în funcție de configurația calculatorului dumneavoastră, acesta poate fi `sda1` în loc de `sdb1`.

2. Așteptați până ce BitDefender Rescue CD pornește calculatorul. Va apărea următoarea fereastră:

Ecran desktop

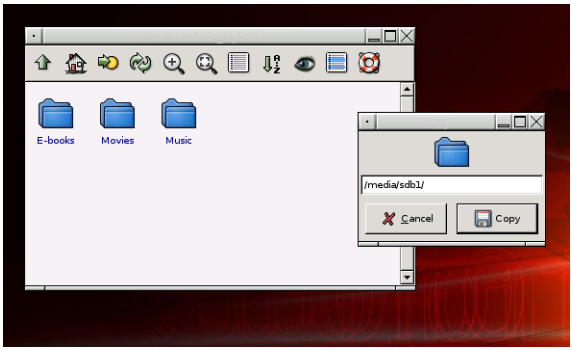
3. Faceți dublu-clic pe partiția unde se află datele pe care vreți să le salvați (de exemplu, `[sda3]`).

   Notă
   Atunci când lucrați cu BitDefender Rescue CD, veți avea de-a face cu nume de partiții de tip Linux. Așadar, `[sda1]` va corespunde probabil partiției `(C:)` din Windows, `[sda3]` partiției `(F:)` și `[sdb1]` stickului de memorie.

   Important
   În cazul în care calculatorul nu a fost închis corect, este posibil ca anumite partiții să nu fi fost montate automat. Pentru a monta o partiție, urmați acești pași:
   a. Faceți dublu-clic pe iconița Terminal Emulator de pe desktop.
   b. Introduceți următoarea comandă:

   ```
   # mount  /media/partition_name
   ```

4. Căutați printre directoare și alegeți-l pe cel dorit. De exemplu, `MyData` care conține subdirectoarele `Movies`, `Music` și `E-books`.
5. Faceți clic-dreapta pe directorul dorit și selectați **Copy**. Va apărea următoarea fereastră.



Salvarea datelor

6. Introduceți `/media/sdb1/` în căsuța de text corespunzătoare și faceți clic pe **Copy**.

   Vă rugăm să țineți cont că în funcție de configurația calculatorului dumneavoastră, acesta poate fi `sda1` în loc de `sdb1`.

38.7. Cum folosesc modul consolă?

Dacă rezoluția ecranului dvs nu este destul de mare pentru a rula interfața grafică, puteți lansa BitDefender Rescue CD în modul consolă. Acesta vă permite să efectuați o scanare completă a calculatorului.

Pentru a rula CD-ul în modul consolă, setați BIOS-ul calculatorului dvs să se lanseze de pe CD, introduceți CD-ul în unitate și reporniți calculatorul. Așteptați să apară ecranul de pornire și selectați **Start knoppix in console mode**.

După ce ați pornit sistemul, urmați instrucțiunile de pe ecran pentru a efectua o scanare completă a calculatorului.

BitDefender detectează partițiile de pe hard disc și actualizează automat baza de date cu semnături de viruși, înainte de începutul scanării. BitDefender va dezinfecta toate fișierele infectate identificate. La final, va fi afișat un jurnal cu rezultatele scanării.

Notă
Procesul de scanare poate dura destul de mult, în funcție de complexitatea scanării.

Vocabular

ActiveX

ActiveX este un mod de scriere a programelor astfel încât să poată fi apelate de celelalte programe și sisteme de operare. Tehnologia ActiveX este utilizată pentru realizarea de pagini Web interactive care se comportă ca niște aplicații și nu ca niște simple pagini statice. Cu elemente de ActiveX, utilizatorii pot răspunde la întrebări, să utilizeze butoane și să interacționeze și în alte moduri cu pagina Web. Controalele ActiveX sunt adesea scrise utilizând limbajul Visual Basic.

Active X este cunoscut pentru lipsa totală de control al securității; experții în securitatea calculatoarelor descurajează utilizarea lui pe Internet.

Adware

Aplicația adware este adesea combinată cu o aplicație gazdă care este oferită gratuit dacă utilizatorul acceptă aplicația adware. Deoarece aplicațiile adware sunt de obicei instalate după ce utilizatorul a fost de acord în prealabil cu un contract de licențiere care explică scopul aplicației, nu este comisă nicio infracțiune.

Totuși, reclamele de tip pop-up pot fi supărătoare, iar în unele cazuri pot afecta performanțele sistemului. De asemenea, informațiile pe care unele dintre aceste aplicații le adună pot cauza motive de îngrijorare utilizatorilor care nu cunosc în întregime termenii din contractul de licențiere.

Arhivă

Un disc, o casetă sau un director care conține fișiere de rezervă.

Un fișier care conține unul sau mai multe fișiere într-un format comprimat.

Backdoor

Reprezintă o gaură de securitate realizată în mod deliberat. Motivația acestor "găuri" nu este întotdeauna malițioasă: unele sisteme de operare, de exemplu, sunt puse în circulație cu conturi privilegiate pentru tehnicienii din service sau de responsabilii cu mentenanță produsului din partea vânzătorului.

Sector de boot

Un sector la începutul fiecărui disc care identifică arhitectura discului (mărimea sectorului, mărimea clusterului și altele). În cazul discurilor de startup, sectorul de boot conține un program care încarcă sistemul de operare.

Virus de boot

Reprezintă un virus care infectează sectorul de boot al unui disc fix sau al unei dischete. Orice încercare de a face boot de pe o dischetă infectată cu un virus de boot va determina virusul să devină activ în memorie. Din acest moment de fiecare dată când veți realiza boot-area sistemului, virusul va deveni activ în memorie.

Browser

Este prescurtarea de la Web Browser, o aplicație utilizată pentru a localiza și încărca pagini de Web. Două din cele mai populare browsere sunt Mozilla Firefox și Microsoft Internet Explorer. Ambele sunt browsere grafice, ceea ce înseamnă că pot afișa atât grafice cât și text. În plus, cele mai moderne browsere pot prezenta informații multimedia, incluzând sunet și animație.

Linie de comandă

Într-o interfață linie de comandă, utilizatorul scrie comenzile în spațiul prevăzut direct pe ecran utilizând limbajul de comandă.

Cookie

Un cookie reprezintă un set de date pe care un server Web îl transmite către un browser atunci când utilizatorul vizitează prima oară site-ul și care este actualizat de fiecare dată când utilizatorul accesează din nou site-ul. Serverul, la fel ca și browserul, salvează informațiile despre utilizator conținute în cookie. Aceste informații sunt stocate sub forma unui fișier text în directoarele de sistem ale browserelor Netscape și Explorer;nu toate browserele suportă cookie. Fișierele cookie stochează informații cum ar fi numele utilizatorului și parola, cât și ce părți din site au fost vizitate. Browserul împarte fiecare cookie doar cu server-ul care l-a generat, celelalte servere le pot citi doar pe cele generate de ele. Unele fișiere cookie sunt programate cu dată de expirare, astfel încât ele vor fi șterse automat după o anumită perioadă de timp.

Drive de disc

Este un dispozitiv care citește date de pe un disc și scrie date pe un disc.

Un drive de hard disc citește / scrie date de pe / pe hard disc.

Un drive de floppy accesează dischetele floppy.

Drive-ele de disc pot fi sau interne (incorporate în interiorul unui calculator) sau externe (plasate într-o locație separată care este conectată la calculator).

Descărcare

Reprezintă copierea (de obicei a unui întreg fișier) de pe o sursă principală pe un dispozitiv periferic. Termenul este adesea utilizat pentru a descrie procesul de copiere a unui fișier de pe un serviciu on-line pe calculatorul unui utilizator. De asemenea se mai poate referi și la copierea unui fișier de pe un server de rețea pe un calculator din rețea.

E-mail

Se referă la poșta electronică. Acesta este un serviciu care transmite mesaje prin intermediul rețelei locale sau globale.

Evenimente

O acțiune sau întâmplare detectată de un program. Evenimentele pot fi acțiuni ale utilizatorului, cum ar fi executarea unui clic cu mouse-ul sau apăsarea unei taste, sau întâmplări în sistem cum ar fi epuizarea memoriei.

Fals pozitiv

Apare atunci când un analizator detectează un fișier ca fiind infectat când de fapt acesta nu este infectat.

Extensie de fișier

Reprezintă porțiunea dintr-un nume de fișier ce urmează după caracterul punct, și care indică tipul de date pe care le stochează fișierul.

Multe sisteme de operare, cum ar fi Unix, VMS, and MS-DOS, utilizează extensii de fișiere. De obicei aceasta este formată din una până la trei caractere (unele sisteme de operare mai vechi nu suportă mai mult de trei). De exemplu: "txt" pentru fișierele text oarecare, "c" pentru fișierele sursă scrise în limbajul C, etc.

Metoda euristică

Reprezintă o metodă bazată pe anumite reguli pentru identificarea de viruși noi. Această metodă de scanare nu se bazează pe semnături de viruși cunoscuți. Avantajul metodei euristice e dat de faptul că nu poate fi păcălită de o nouă variantă a unui virus deja existent. Totuși ocazional poate raporta un cod suspicios în programe normale, generând așa-numitul "fals pozitiv".

IP

Internet Protocol - Un protocol rutabil din suita protocoalelor TCP / IP căruia i se atribuie adresarea IP, rutarea, fragmentarea cât și reasamblarea pachetelor IP.

Applet-uri Java

Reprezintă un program Java care este proiectat să ruleze doar pe pagini web. Pentru a utiliza un applet pe o pagină web, trebuie specificate numele applet-ului și mărimea acestuia. Când este accesată o pagină web, browser-ul descarcă applet-ul de pe un server și îl rulează pe mașina utilizatorului (clientul). Applet-urile diferă de aplicații prin aceea că sunt guvernate de un protocol de securitate strict.

Astfel că, deși pot rula pe calculatorul unui utilizator, ele nu pot citi sau scrie date pe aceste calculatoare. Applet-urile sunt restricționate de domeniul de care aparțin în ceea ce privește scrierea și citirea datelor.

Virus de macro

Un tip de virus informatic este acela inclus ca macro într-un document. Multe aplicații cum ar fi de exemplu Microsoft Word și Excel suportă limbaje macro puternice.

Aceste limbaje permit încapsularea de macro-uri în documente și execută aceste macro-uri de fiecare dată când este deschis documentul.

Client de mail

Un client de mail este o aplicație care vă permite să trimiteți și să recepționați mesaje.

Memorie

Reprezintă arii de stocare a datelor din interiorul calculatorului. Termenul de memorie desemnează locul de stocare a datelor pe chipuri și pe cel al cuvintelor pe casete sau cd-uri audio. Fiecare calculator dispune de o anumită capacitate de memorie fizică, referită de obicei prin memorie principală sau RAM.

Metoda ne-euristică

Această metodă de scanare se bazează pe semnături specifice de viruși. Avantajul metodelor ne-euristice constă în aceea că scannerul nu poate fi "păcălit" de ceea ce poate părea un virus și din acest motiv nu generează fals pozitiv.

Programe împachetate

Reprezintă un fișier în format comprimat. Multe din sistemele de operare și aplicații conțin comenzi care vă dau posibilitatea de a împacheta un fișier astfel încât să ocupe mai putină memorie. De exemplu, să presupunem că aveți un fișier text care conține zece caractere reprezentând spații. În mod normal, acesta ar necesita zece biți de memorie pentru a fi stocați.

Totuși, un program care împachetează fișiere va înlocui caracterele de spațiu printr-un caracter reprezentând spațiu, urmat de un număr care reprezintă numărul de spații care este înlocuit. În acest caz, cele zece caractere reprezentând spațiu ar necesita doar doi biți. Aceasta este doar un exemplu de comprimare - există multe alte metode în afară de aceasta.

Cale

Reprezintă direcția exactă către un fișier de pe un calculator. Această direcție este specificată utilizând sistemul ierarhic de organizare a fișierelor de sus în jos.

Ruta între două puncte, cum ar fi de exemplu canalul de comunicație între două computere.

Phishing

Reprezintă acțiunea de a trimite un e-mail către un utilizator, pretinzând a fi o companie legitimă, în încercarea de a păcăli utilizatorul să furnizeze informații confidențiale ce vor fi folosite la furtul identității. E-mailul îndreaptă utilizatorul către un site Web unde acesta este rugat să actualizeze informații personale, cum ar fi parole și numere de card de credit, de asigurări sociale și de conturi bancare pe care compania respectivă deja le are. Site-ul Web este însă fals și folosit pentru a fura informațiile despre utilizator.

Virus polimorf

Reprezintă un virus care își schimbă forma cu fiecare fișier pe care îl infectează. Din cauză că nu au un tipar binar consistent, asemenea viruși sunt greu de identificat.

Port

Reprezintă o interfață a unui calculator la care se poate conecta un dispozitiv. Calculatoarele personale dispun de diferite tipuri de porturi. Există porturi interne pentru conectarea hard discurilor, monitoarelor și tastaturilor. Există porturi externe pentru conectarea modemului, imprimantei, mouse-ului și a altor dispozitive periferice.

În rețelele TCP / IP și UDP acestea reprezintă un punct terminus al unei conexiuni logice. Numărul portului identifică ce tip de port este. De exemplu, portul 80 este utilizat pentru traficul HTTP.

Fișier de raport

Reprezintă un fișier care listează acțiunile care au avut loc. BitDefender menține un fișier log (jurnal) în care sunt listate obiectele care au fost scanate, numele fișierelor, numărul de arhive și fișiere scanate, câte fișiere infectate și suspecte au fost găsite.

Rootkit

Un rootkit este un set de unelte soft ce oferă acces la nivel de administrator în interiorul unui sistem. Termenul a fost utilizat pentru prima oară pentru sistemele de operare UNIX și se referea la unelte recompilate ce furnizau intrușilor drepturi administrative, permițându-le să își ascundă prezența astfel încât să nu poată fi văzuți de către administratorii de sistem.

Rolul principal al rootkiturilor este de a ascunde procese, fișiere, loginuri și jurnale. Acestea pot de asemenea să intercepteze date de la terminale, conexiuni la rețea sau perifice dacă sunt dotate cu softul adecvat.

Rootkiturile nu sunt malițioase prin natură. De exemplu, sistemele și chiar unele aplicații ascunde fișiere critice utilizând rootkituri. Totuși, ele sunt folosite în general pentru a ascunde aplicații malițioase sau prezența intrușilor în sistem. În combinație cu aplicații malițioase, rootkiturile constituie o mare amenințare pentru securitatea și integritatea sistemului. Acestea pot monitoriza traficul, crea porți de acces în sistem ("backdoors"), altera fișiere și jurnale și evita detecția.

Script

Un alt termen pentru fișiere macro sau de tip "bat", un script reprezintă o listă de comenzi care pot fi executate fără intervenția utilizatorului.

Spam

Termen ce acoperă întreagă gamă a mesajelor electronice nesolicitate.

Spyware

Reprezintă orice software care strânge informații despre utilizator prin intermediul conexiunii la Internet fără știrea acestuia, de obicei în scopuri publicitare. Aplicațiile spyware sunt de obicei primite ca parte ascunsă a unui program de tip freeware sau shareware, ce poate fi descărcat de pe Internet; totuși, trebuie știut că majoritatea aplicațiilor de tip shareware și freeware nu

conțin aplicații spyware. Odată instalată, aplicația spyware monitorizează activitatea utilizatorului pe Internet și transmite pe ascuns informații altei persoane. Aplicațiile spyware pot aduna, de asemenea, informații despre adresele e-mail și chiar parole și numere de carduri de credit.

Asemănarea dintre spyware și un cal troian este faptul că utilizatorul instalează aplicația fără voia sa atunci când instalează altceva. Un mod obișnuit de a deveni victima unei aplicații spyware este de a descărca prin rețelele peer-to-peer anumite produse de schimb de fișiere care sunt disponibile astăzi.

Pe lângă problemele legate de etică și intimitate, aplicația spyware fură de la utilizator atât prin folosirea memoriei calculatorului cât și a lungimii de bandă deoarece trimite informații înapoi la sursă prin intermediul conexiunii la Internet a utilizatorului. Deoarece folosesc memorie și resurse ale sistemului, aplicațiile spyware pot conduce la blocarea sistemului sau la instabilitate generală.

Elemente din startup

Orice fișier plasat în acest director se va deschide de fiecare dată când calculatorul este pornit. De exemplu, un sunet care se va auzi atunci când este pornit calculatorul sau chiar aplicații sunt considerate elemente de startup. În mod normal, un alias al programului este plasat în acest director, și nu direct fișierul.

Bara de sistem

Introdusă odată cu apariția sistemului Windows 95, bara de sistem este plasată în taskbar-ul de Windows (situat lângă ceas) și conține iconițe pentru accesul rapid la aplicații sistem cum ar fi cele legate de fax, imprimantă, modem, volum, și altele. Executați dublu-clic cu mouse-ul pe o iconiță pentru a vizualiza și accesa elementele.

TCP/IP

Transmission Control Protocol/Internet Protocol - Un set de protocoale de rețea folosite în mod larg în domeniul Internet și care asigură comunicarea între rețelele de calculatoare interconectate având arhitecturi hardware și sisteme de operare diferite. TCP/IP include standarde referitoare la realizarea comunicării între calculatoare cât și convenții folosite în conectarea rețelelor și rutării traficului.

Troian

Este un program distructiv care este mascat sub forma unei aplicații benigne. Spre deosebire de viruși, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cei mai mascați troieni este acela care pretinde că elimină virușii de pe computerul dumneavoastră, dar în loc de aceasta, introduce viruși pe calculatorul dumneavoastră.

Termenul provine de la o poveste din opera "Iliada" lui Homer, în care grecii oferă dușmanilor lor, troienii, în semn de pace un cal gigantic de lemn. Dar după ce troienii aduc acest cal în interiorul orașului lor, din interiorul calului ies

o mulțime de soldați greci, care deschid porțile cetății, permițându-le celorlalți soldați greci să pătrundă în oraș și să captureze Troia.

Actualizare

O versiune nouă de produs hardware sau software proiectat să înlocuiască o versiune mai veche a aceluiași produs. În afară de acesta, rutinele de instalare verifică dacă există instalată pe calculatorul dumneavoastră o altă versiune mai veche; dacă nu, nu puteți instala actualizarea.

BitDefender dispune de modulul său propriu care realizează actualizarea automatică sau manuală.

Virus

Reprezintă un program sau o bucată de cod care se încarcă pe calculator fără știrea dumneavoastră și rulează independent de voința dumneavoastră. Cea mai mare parte a virușilor se pot și înmulți. Toți virușii informatici sunt creați de om. Un simplu virus care poate realiza copii ale sale este relativ simplu de produs. Chiar și un asemenea virus este periculos întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. Un virus și mai periculos este acela care este capabil să se răspândească în rețea și poate să treacă de sistemele de securitate.

Semnătură de virus

Reprezintă tiparul binar al unui virus, utilizat de un program antivirus pentru detecția și eliminarea virusului.

Vierme

Reprezintă un program care se autopropagă în interiorul unei rețele, reproducându-se pe măsură ce se răspândește. Nu se poate atașa la alte programe.