bitdefender

TOTAL SECURITY 2009

Manual de utilizare

bitdefender

Copyright© 2008 BitDefender

BitDefender Total Security 2009

Manual de utilizare

Publicat 2008.08.26

Copyright© 2008 BitDefender

Termeni legali

Toate drepturile rezervate. Nicio parte a acestui manual nu va putea fi reprodusă sau transmisă sub nicio formă şi prin niciun mijloc, fie el electronic sau mecanic, inclusiv fotocopiere, înregistrare, sau orice sistem de stocare şi recuperare de date, fără acordul scris al BitDefender, cu excepția includerii unor scurte citate în recenzii. Conținutul manualului nu poate fi modificat în niciun fel.

Avertisment şi declinarea responsabilității. Acest produs şi documentația aferentă sunt protejate de dreptul de autor. Informațiile incluse în acest document sunt furnizate "ca atare", fără nicio garanție. Deşi s-au luat toate măsurile de prevedere în momentul alcătuirii acestui document, autorii săi nu vor fi în niciun fel ținuți responsabili față de nicio persoană fizică sau juridică pentru pierderi sau daune cauzate sau care se presupune a fi fost cauzate, direct sau indirect, de informațiile cuprinse în acest material.

Acest manual conține linkuri către pagini web aparținând unor terți care nu se află sub controlul BitDefender; prin urmare, BitDefender nu este responsabilă pentru conținutul respectivelor pagini. Dacă accesați o astfel de pagină web, veți face acest lucru pe propria răspundere. BitDefender oferă aceste linkuri exclusiv pentru uşurarea consultării şi includerea linkului nu presupune faptul că BitDefender susține sau îşi asumă responsibilitatea pentru conținutul acestor pagini web.

Mărci înregistrate. Acest manual poate conține nume de mărci înregistrate. Toate mărcile comerciale înregistrate sau neînregistrate din acest document aparțin exclusiv proprietarilor acestora şi sunt redate ca atare.

bitdefender

Cuprins

Licență și garanție

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

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

Acest Contract de licență reprezintă o convenție legală între dumneavoastră (ca persoană fizică sau persoană juridică utilizator final) şi BITDEFENDER pentru utilizarea produsului software identificat mai sus, aparținând BITDEFENDER, care include softul propriu-zis şi serviciile, şi poate include, medii de informație asociate, materiale tipărite şi documentație "on line" sau electronică (referite în continuare ca "BitDefender"). Toate acestea sunt protejate de legislația internațională privind drepturile de autor şi proprietatea intelectuală, precum şi 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 şi nu utilizați produsul BitDefender.

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

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

APLICAȚIA SOFTWARE. Puteți instala şi 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 şi care nu furnizează servicii pentru rețele. Fiecare utilizator principal poate instala acest soft pe un singur calculator şi 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 şi va continua doar până la sfârşitul 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, înlocuieşte şi/sau completează produsul care reprezintă baza dreptului dumneavoastră de a beneficia de actualizarea de produs. Puteți utiliza produsul rezultat în urma actualizării numai în concordantă 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 şi nu poate fi separat pentru utilizarea sa de către mai mulți utilizatori decât numărul de licențe. Termenii şi condițiile acestei licențe înlocuiesc şi prevalează orice alte înțelegeri care ar fi putut exista între dumneavoastră şi BITDEFENDER privind produsul original sau produsul rezultat ca urmare a actualizării.

COPYRIGHT. Toate drepturile, titlurile şi beneficiile ce țin de BitDefender (inclusiv, dar fără a se limita la orice imagine, fotografie, animație, video, audio, muzică, text şi cod, încorporate în produsul BitDefender), toate materialele tipărite care însoțesc produsul şi orice copie a produsului BitDefender sunt proprietatea BITDEFENDER. BitDefender este protejat de legile şi tratatele internaționale privind drepturile de autor şi 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 şi 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 cerintelor 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 ŞI CONDIȚII IMPLICITE, INCLUZÂND, FĂRĂ LIMITARE, GARANȚIILE IMPLICITE ALE VANDABILITĂȚII, UTILIZĂRII ÎNTR-UN ANUMIT SCOP, TITLULUI, NON-INTERFERENȚEI, ACURATEȚEI DATELOR, A CONȚINUTULUI INFORMAȚIONAL, INTEGRĂRII SISTEMULUI ŞI NEÎNCĂLCĂRII DREPTURILOR UNOR TERȚE PĂRȚI PRIN FILTRAREA, DEZACTIVAREA SAU ÎNDEPĂRTAREA SOFTULUI ACESTORA, A APLICAȚIILOR SPYWARE, ADWARE, A FIŞIERELOR 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 îşi asumă riscul legat de calitatea şi 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. ÎN NICIUN CAZ, RESPONSABILITATEA BITDEFENDER NU VA DEPĂŞI PREȚUL DE ACHIZIȚIE AL PRODUSULUI BITDEFENDER. Declarațiile de limitare şi 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 ŞI NU ESTE PROIECTAT SAU DESTINAT UTILIZĂRII ÎNTR-UN MEDIU CU GRAD MARE DE RISC ŞI 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 EROARI AR PUTEA CAUZA MOARTEA SAU RĂNIREA GRAVĂ A UNOR PERSOANE SAU DAUNE ALE PROPRIETĂȚII.

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

Prețurile, costurile şi sumele de bani pentru utilizarea BitDefender pot fi modificate fără să fiți anunțat în prealabil.

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

BitDefender şi 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 şi condițiile privind confidențialitatea şi restricțiile de utilizare vor rămâne în vigoare şi după orice anulare a licenței.

BITDEFENDER poate revizui aceşti 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 şi 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.

Contactați BitDefender la strada Preciziei, nr. 24, West Gate Park, Clădirea H2, sector 6, Bucureşti, România, la telefon +40-21-2063470 sau pe adresa de e-mail: sales@bitdefender.ro.

Prefață

Acest manual se adresează tuturor utilizatorilor care au ales **BitDefender Total Security 2009** ca soluție de securitate pentru calculatoarele personale. Informațiile incluse în acest manual sunt destinate nu numai utilizatorilor avansați, ci şi oricărei persoane care poate lucra în sistemul Windows.

Acest manual vă prezintă **BitDefender Total Security 2009**, Compania şi echipa care l-au dezvoltat, vă ghidează în timpul procesului de instalare a produsului şi vă învață cum să-l configurați. Veți afla cum să utilizați **BitDefender Total Security 2009**, cum să-l actualizați, testați şi personalizați. Veți învăța cum să obțineți beneficii maxime din BitDefender.

Vă dorim o lectură plăcută şi utilă.

1. Convenții utilizate în manual

1.1. Convenții tipografice

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

Aspect	Descriere
`sample syntax`	Exemplele de sintaxă sunt tipărite cu caractere `monospaţiate`.
http://www.bitdefender.com	Linkurile URL indică locații externe, pe serverele http sau ftp.
support@bitdefender.com	Adresele de e-mail sunt inserate în text ca adrese de contact.
“Prefață” (p. xvi)	Acesta este un link intern, către o locație din document.
`filename`	Numele fişierelor şi ale directoarelor sunt tipărite cu caractere `monospaţiate`.
option	Toate opțiunile produsului sunt tipărite cu caractere **aldine**.

Aspect	Descriere
`sample code listing`	Liniile de cod sunt tipărite cu caractere monospaţiate.

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. Deşi 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 şi nu este recomandat să-l ocoliți. De obicei, aici sunt furnizate 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 şi să înțelegeți despre ce este vorba, deoarece este descris 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. Instrucțiuni de instalare pas cu pas a BitDefender pe o stație de lucru. Acesta este un ghid complet pentru instalarea **BitDefender Total Security 2009**. Începând cu cerințele pentru o instalare corectă, sunteți ghidat de-a lungul întregului proces de instalare. La sfârşit este descrisă şi procedura de dezinstalare a BitDefender, pentru cazul în care doriți să faceți acest lucru.

Administrare elementară. Descriere a administrării elementare a BitDefender.

Administrare avansată. Aceasta este o prezentare detaliată a tipurilor de protecție oferite de BitDefender. Sunteți învățat cum să configurați şi să utilizați toate modulele BitDefender astfel încât să vă protejați eficient calculatorul împotriva oricăror amenințări (aplicații malițioase, spam, hackeri, conținut inadecvat şi altele).

Obținere ajutor. Unde să căutați şi unde să cereți ajutor în cazul în care apar situații neprevăzute.

BitDefender Rescue CD. Aceasta este o descriere a BitDefender Rescue CD. Vă ajută să înțelegeți şi să utilizați funcțiile oferite de acest CD de boot.

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

3. Comentarii

Vă invităm să ne ajutați să îmbunătățim acest manual. Am testat şi 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

1. Cerințe de sistem

Puteți instala BitDefender Total Security 2009 doar pe calculatoare pe care rulează următoarele sisteme de operare:

- Windows XP cu Service Pack 2 (32/64 biți) sau superior
- Windows Vista (32/64 biți) sau Windows Vista cu Service Pack 1
- Windows Home Server

Înainte de instalare, asigurați-vă că sistemul dumneavoastră îndeplineşte cerințele hardware şi software minime.

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

1.1. Cerințe hardware

Pentru Windows XP

- Procesor de 800 MHz sau superior
- 256 MB memorie RAM (1 GB recomandat)
- 210 MB spațiu disponibil pe hard disc (250 MB recomandat)

Pentru Windows Vista

- Procesor de 800 MHz sau superior
- 512 MB memorie RAM (1 GB recomandat)
- 210 MB spațiu disponibil pe hard disc (250 MB recomandat)

Pentru Windows Home Server

- Procesor de 800 MHz sau superior
- 512 MB memorie RAM (1 GB recomandat)
- 210 MB spațiu disponibil pe hard disc (250 MB recomandat)

1.2. Cerințe software

- Internet Explorer 6.0 (sau mai recent)
- .NET Framework 1.1 (disponibil şi în kitul de instalare)

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

- Microsoft Outlook 2000 / 2002 / 2003 / 2007
- Microsoft Outlook Express
- Microsoft Windows Mail
- Thunderbird 1.5 şi 2.0

Protecția antiphishing este oferită doar pentru:

- Internet Explorer 6.0 sau mai recent
- Mozilla Firefox 2.0
- Yahoo! Messenger 8.1
- Windows Live (MSN) Messenger 8.5

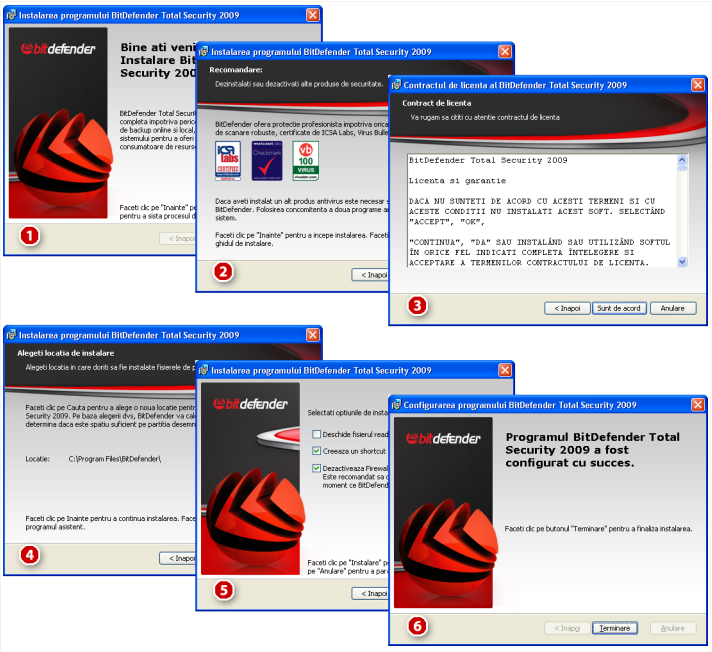
Criptarea mesageriei instant (IM) este oferită doar pentru:

- Yahoo! Messenger 8.1
- Windows Live (MSN) Messenger 8.5

2. Instalarea BitDefender

Localizați fișierul de instalare şi faceți dublu-clic. Astfel, va fi lansat programul asistent care vă va ghida pe parcursul procesului de instalare.

Înainte de lansarea programului asistent, BitDefender va căuta versiuni mai noi ale fișierului de instalare. Dacă o versiune mai nouă este disponibilă, vi se va cere să o descărcați. Faceți clic pe **Da** pentru a descărca versiunea mai nouă sau pe **Nu** pentru a continua instalarea utilizând versiunea din fișierul de instalare.



Etapele instalării

Urmați aceşti paşi pentru a instala BitDefender Total Security 2009:

1. Faceți clic pe **Înainte** pentru a continua sau pe **Anulare** dacă doriți să părăsiți procesul de instalare.
2. Faceți clic pe **Înainte**.

   BitDefender Total Security 2009 vă alertează dacă aveți alte produse antivirus instalate pe calculatorul dumneavoastră. Faceți clic pe **Şterge** 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 acelaşi timp, pe acelaşi calculator, provoacă în general instabilitatea sistemului de operare.

3. Vă rugăm să citiți cu atenție Contractul de licență şi să faceți clic pe **Accept**.

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

4. În mod implicit, BitDefender Total Security 2009 va fi instalat în `C:\Program Files\BitDefender\BitDefender 2009`. Dacă doriți să schimbați calea de instalare, faceți clic pe butonul **Caută** şi selectați directorul în care doriți să fie instalat BitDefender.

   Faceți clic pe **Înainte**.

5. Selectați opțiuni referitoare la procesul de instalare. Unele dintre acestea vor fi selectate implicit:
   - **Deschide fişierul readme** - pentru a deschide fişierul readme la sfârşitul instalării.
   - **Creează un shortcut pe desktop** - pentru a crea pe desktop o scurtătură (shortcut) către BitDefender Total Security 2009 la finalizarea instalării.
   - **Scoate CD când instalarea este finalizată** - pentru a scoate CD-ul din unitate la sfârşitul instalării; această opțiune apare atunci când instalați produsul de pe CD.
   - **Dezactivează Firewallul Windows** - pentru a dezactiva aplicația Windows Firewall.

Important
Vă recomandăm să dezactivați Windows Firewall deoarece BitDefender Total Security 2009 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 doar pe Windows Vista.

Faceți clic pe **Instalare** pentru a lansa instalarea programului. Dacă nu este deja instalat, BitDefender va instala mai întâi .NET Framework 1.1.

Aşteptați până când instalarea este finalizată.

6. Faceți clic pe **Finalizare**. Vi se va cere să reporniți sistemul pentru a finaliza procesul de instalare. Faceți acest lucru cât mai curând posibil.

Important
După finalizarea instalării şi repornirea calculatorului, vor apărea un program asistent de înregistrare şi un program asistent de configurare. Urmați paşii acestor programe asistent pentru a înregistra şi configura BitDefender Total Security 2009 şi 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 2009`.

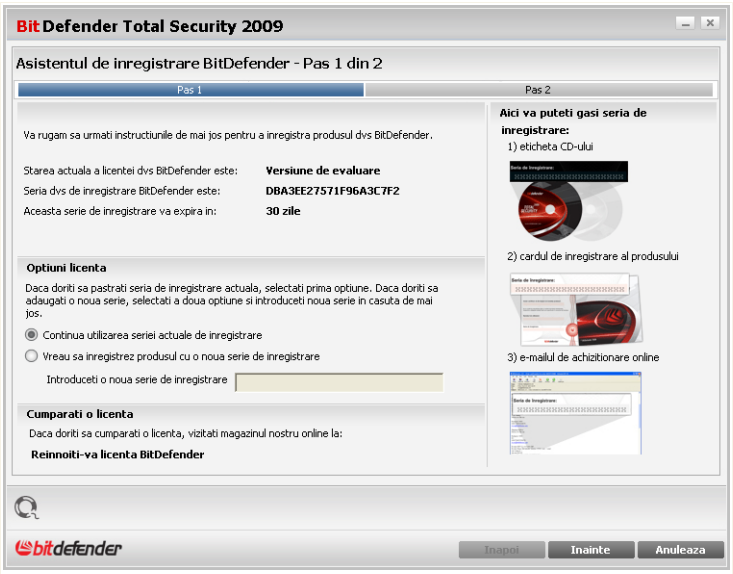
2.1. Asistentul de înregistrare

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

Contul BitDefender oferă acces la suport tehnic gratuit, oferte speciale şi 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 **Anulare**. Puteți deschide programul asistent de înregistrare oricând doriți, făcând clic pe linkul **Înregistrează**, situat în partea de jos a ferestrei principale a produsului.

2.1.1. Pasul 1/2 - Înregistrați BitDefender Total Security 2009



Înregistrare

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

Pentru a evalua produsul în continuare, selectați **Continuă evaluarea produsului**.

Pentru a înregistra BitDefender Total Security 2009:

1. Selectați **Vreau să înregistrez produsul cu o nouă serie**.
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 şi a cumpăra una.

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

2.1.2. Pasul 2/2 - Creați un cont BitDefender

Creare cont

Dacă nu doriți să creați un cont BitDefender în acest moment, selectați **Sari peste înregistrare** şi faceți clic pe **Finalizare** Altfel, continuați în funcție de situația dumneavoastră actuală:

- “Nu am un cont BitDefender” (p. 9)
- “Deja am un cont BitDefender” (p. 9)

Nu am un cont BitDefender

Selectați **Creează un nou cont BitDefender** şi furnizați informațiile cerute. Informațiile furnizate aici vor rămâne confidențiale.

- **E-mail** - introduceți adresa de e-mail.
- **Parolă** - introduceți o parolă pentru contul dumneavoastră BitDefender. Parola trebuie să conțină minim şase caractere.
- **Reintroduceți parola** - introduceți parola din nou.
- **Prenume** - introduceți prenumele dumneavoastră.
- **Nume** - introduceți numele dumneavoastră de familie.
- **Țara** - selectați țara în care locuiți.

Notă
Folosiți adresa de e-mail şi parola pentru a vă accesa contul dumneavoastră la adresa http://myaccount.bitdefender.com.

Pentru a crea un cont trebuie mai întâi să vă activați adresa de e-mail. Verificați-vă adresa de e-mail şi urmați instrucțiunile din e-mailul trimis de serviciul de înregistrare BitDefender.

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

- **Vreau sa primesc toate mesajele de la BitDefender**
- **Vreau sa primesc numai cele mai importante mesaje**
- **Nu vreau sa primesc niciun mesaj**

Faceți clic pe **Finalizare**.

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 dumneavoastră.

Dacă aveți deja un cont activ, dar BitDefender nu l-a detectat, selectați **Accesează un cont BitDefender existent** şi furnizați adresa de e-mail şi parola contului dumneavoastră.

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

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

- **Vreau sa primesc toate mesajele de la BitDefender**
- **Vreau sa primesc numai cele mai importante mesaje**
- **Nu vreau sa primesc niciun mesaj**

Faceți clic pe **Finalizare**.

2.2. Asistentul de configurare

Odată ce ați finalizat programul asistent de înregistrare, va apărea un program asistent de configurare. Programul asistent vă ajută să configurați anumite module ale produsului şi să setați BitDefender să execute sarcini importante de securitate.

Nu este obligatoriu să urmați paşii programului asistent. Totuşi, vă recomandăm să faceți acest lucru pentru a economisi timp şi pentru a vă asigura că sistemul dumneavoastră nu era infectat înainte de a instala BitDefender Total Security 2009.

Notã

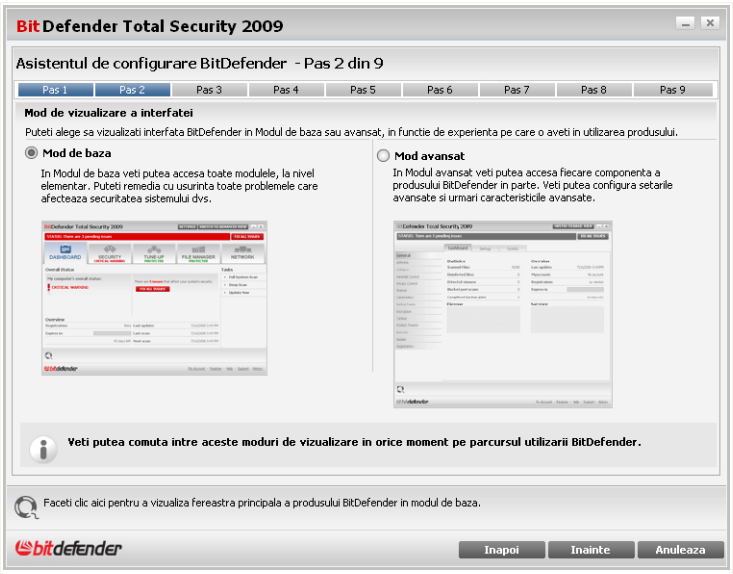
Dacă nu doriți să urmați acest program asistent, faceți clic pe **Anulare**. BitDefender vă va informa despre componentele care trebuie configurate atunci când deschideți fereastra principală a produsului.

2.2.1. Fereastra de întâmpinare

Fereastra de întâmpinare

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

2.2.2. Pasul 2/9 - Selectați modul de vizualizare



Moduri de vizualizare

Alegeți între cele două moduri de vizualizare ale interfeței în funcție de experiența dumneavoastră în utilizarea BitDefender:

- **Modul de bază.** Interfață simplă, adecvată utilizatorilor începători şi celor care doresc să utilizeze doar sarcinile de bază şi să rezolve uşor problemele care apar. Trebuie doar să urmăriți avertismentele şi alertele BitDefender şi să rezolvați problemele care apar.
- **Modul avansat.** Interfață avansată, adecvată utilizatorilor care doresc să configureze produsul în totalitate. Puteți configura fiecare componentă a produsului şi efectua sarcini avansate.

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

2.2.3. Pasul 3/9 - Configurați rețeaua BitDefender

Configurarea rețelei BitDefender

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

Dacă doriți ca acest calculator să fie parte a rețelei BitDefender, urmați aceşti paşi:

1. Selectați **Vreau să fac parte din rețeaua personală BitDefender**.
2. Introduceți aceeaşi parolă administrativă în fiecare dintre câmpurile editabile.

Important

Parola permite unui administrator să administreze acest produs BitDefender de la un alt calculator.

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

2.2.4. Pasul 4/9 - Configurați controlul identității

Configurare Control identitate

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, căutând anumite şiruri de caractere (de exemplu, numărul cardului dumneavoastră de credit). Dacă există o concordanță, site-ul web, e-mailul sau mesajul instant respectiv este blocat.

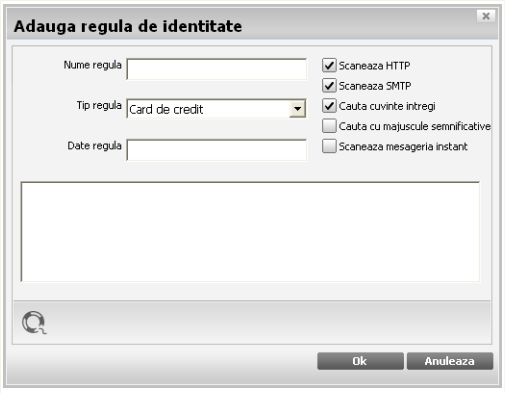
Dacă doriți să utilizați Controlul identității, urmați aceşti paşi:

1. Selectați **Vreau să utilizez Controlul identității**.
2. Creați reguli pentru a vă proteja datele confidențiale. Pentru mai multe informații, consultați “Crearea regulilor Controlului de identitate” (p. 15).
3. Daca este nevoie, definiți excepții specifice de la regulile pe care le-ați creat. Pentru mai multe informații, consultați “Specificarea excepțiilor Controlului identității” (p. 16).

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

Crearea regulilor Controlului de identitate

Pentru a crea o regulă de Control de identitate, faceți clic pe **Adaugă**. Va apărea fereastra de configurare.



Regulă control identitate

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.).
- **Date 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 greşită a mesajelor şi a paginilor web.

Puteți alege să aplicați regula doar dacă datele protejate apar ca şir independent sau ținând cont de majuscule şi minuscule.

Pentru a identifica cu uşurinţă informaţiile blocate de către regulă, furnizaţi o descriere detaliată a regulii în căsuţa editabilă.

Pentru a specifica tipul de trafic care să fie scanat, configuraţi aceste opţiuni:

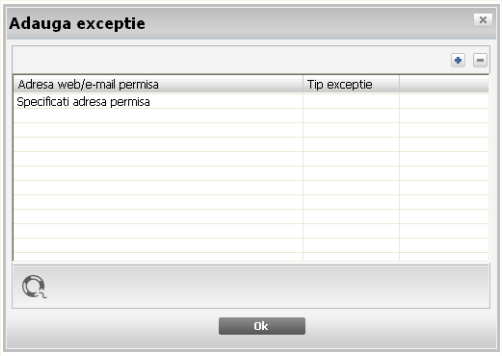
- **Scanează HTTP** - scanează traficul HTTP (web) şi blochează la ieşire toate datele care corespund unei reguli.
- **Scanează SMTP** - scanează traficul SMTP (mail) şi blochează trimiterea mesajelor e-mail care corespund unei reguli.
- **Scanează mesageria instant** - scanează traficul de mesagerie instant şi blochează trimiterea mesajelor instant care corespund unei reguli.

Faceţi clic pe **OK** pentru a adăuga regula.

Specificarea excepţiilor Controlului identităţii

În unele cazuri, este nevoie să definiţi excepţii la anumite reguli de identitate. Consideraţi cazul în care creaţi 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 doriţi, de exemplu, să cumpăraţi o pereche de pantofi prin intermediul unui magazin online (care ştiţi că este securizat), va trebui să specificaţi o excepţie de la regula respectivă.

Pentru a deschide fereastra unde puteţi gestiona excepţiile, faceţi clic pe **Excepţii**.



Excepţii Control identitate

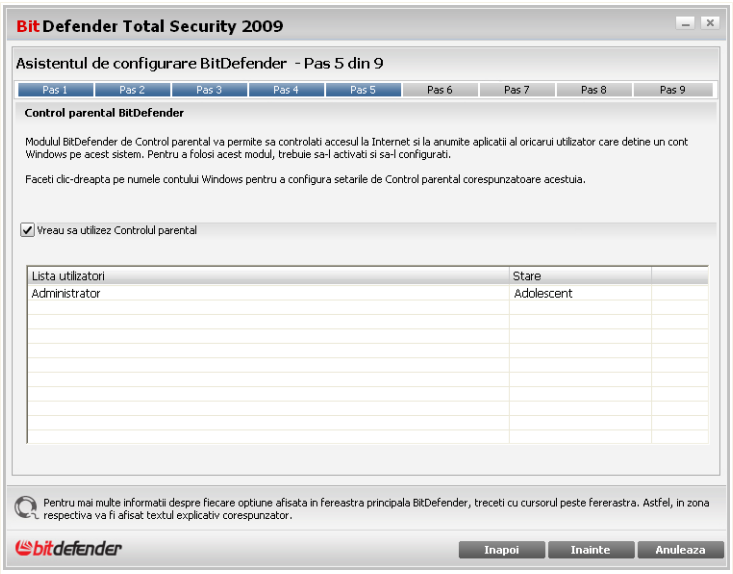
Pentru a adăuga o excepție, urmați aceşti paşi:

1. Faceți clic pe butonul **Adaugă** pentru a adăuga o nouă înregistrare în tabel.
2. Faceți dublu-clic pe **Specificați adresa permisă** şi furnizați adresa web sau adresa de e-mail pe care doriți să o adăugați ca excepție.
3. Faceți dublu-clic pe **Alegeți tipul** şi alegeți din meniu opțiunea corespunzătoare tipului de adresă furnizată anterior.
   - Dacă ați specificat o adresă web, selectați **HTTP**.
   - Dacă ați specificat o adresă de mail, selectați **SMTP**.

Pentru a şterge o excepție, selectați-o şi faceți clic pe butonul **Şterge**.

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

2.2.5. Pasul 5/9 - Configurați controlul parental



Configurare Control parental

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

Dacă doriți să utilizați Controlul parental, urmați aceşti paşi:

1. Selectați **Vreau să utilizez Controlul parental**.
2. Faceți clic-dreapta pe numele fiecărui cont Windows şi selectați profilul de Control parental care să fie aplicat.

Profil	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.

Profil	Descriere
Adolescent	Oferă acces web restricționat, conform setărilor recomandate pentru utilizatori având vârsta între 14 şi 18 ani. Paginile web cu conținut sexual sau pornografic sunt blocate.
Adult	Oferă acces nerestricționat la toate paginile web indiferent de conținutul acestora.

Notă

Pentru a configura complet sau a dezactiva Controlul parental pentru anumite conturi Windows, deschideți fereastra BitDefender, comutați pe Modul avansat şi mergeți la Control parental. 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 şi mesajele instant care conțin anumite cuvinte cheie.
- jocuri, aplicații de chat, partajare de fişiere şi altele.
- mesaje instant trimise de alte contacte IM decât cele permise.

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

2.2.6. Pasul 6/9 - Configurați raportarea virușilor

Setări raportare viruși

BitDefender poate trimite Laboratorului BitDefender rapoarte anonime referitoare la viruşii identificați în calculatorul dumneavoastră pentru a ține evidența noilor viruşi.

Puteți configura următoarele opțiuni:

- **Trimite raport viruşi** - trimite Laboratorului BitDefender rapoarte referitoare la viruşii identificați în calculatorul dumneavoastră.
- **Activează Detecția epidemiilor virale de către BitDefender** - trimite Laboratorului BitDefender rapoarte referitoare la potențiale epidemii virale.

Notă
Rapoartele nu conțin date confidențiale, cum ar fi numele dumneavoastră sau adresa IP, şi nu vor fi folosite în scopuri comerciale.

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

2.2.7. Pasul 7/9 - Selectați sarcinile ce vor fi rulate

Selectare sarcini

Configurați BitDefender Total Security 2009 să execute sarcini importante privind securitatea sistemului dumneavoastră. Următoarele opțiuni sunt disponibile:

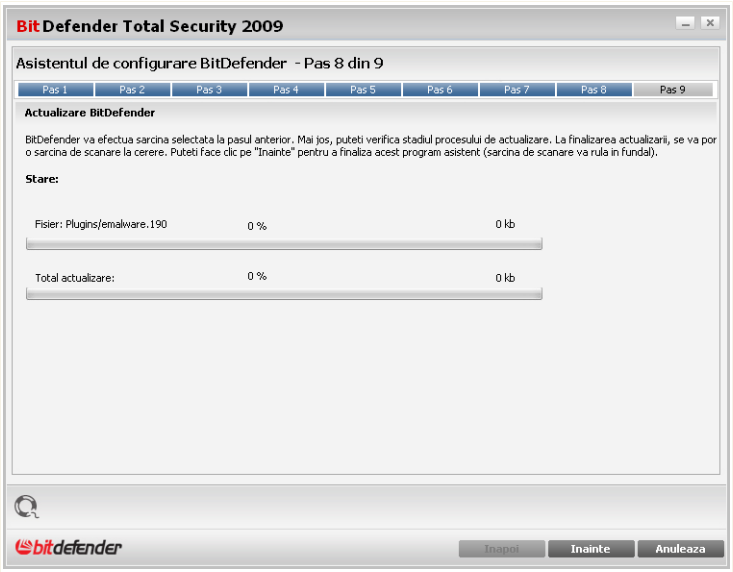
- **Actualizează motoarele BitDefender (poate fi necesară repornirea sistemului)** - în timpul pasului următor va fi efectuată o actualizare a motoarelor BitDefender pentru a vă proteja sistemul împotriva celor mai noi amenințări.
- **Rulează o scanare rapidă a sistemului (poate fi necesară repornirea sistemului)** - în timpul pasului următor va fi efectuată o scanare rapidă a sistemului ce va permite BitDefender să se asigure că fişierele dumneavoastră din directoarele `Windows` şi `Program Files` nu sunt infectate.
- **Planifică o scanare completă a sistemului în fiecare zi la 2 AM** - rulează o scanare completă a sistemului în fiecare zi la ora 2.

Important
Vă recomandăm să păstrați aceste opțiuni selectate înainte de a trece la pasul următor pentru a asigura securitatea sistemului dumneavoastră.

Dacă selectați doar ultima opțiune sau nicio opțiune, veți sări peste pasul următor.

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

2.2.8. Pasul 8/9 - Așteptați finalizarea sarcinilor



Stare sarcini

Aşteptați ca sarcinile să fie finalizate. Puteți vedea starea sarcinilor selectate în pasul anterior.

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

2.2.9. Pasul 9/9 - Finalizare

Finalizare

Selectați **Deschide contul meu BitDefender** pentru a vă accesa contul BitDefender. Este necesară o conexiune la Internet.

Faceți clic pe **Finalizare**.

3. Repararea sau dezinstalarea BitDefender

Dacă doriți să reparați sau să dezinstalați **BitDefender Total Security 2009**, urmați calea din meniul Start al Windows: **Start** → **Programe** → **BitDefender 2009** → **Reparare sau Dezinstalare**.

Vi se va solicita să confirmați alegerea făcând clic pe butonul **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 şi, după repornire, faceți clic pe **Instalare** pentru a reinstala BitDefender Total Security 2009.

  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 viruşilor, a aplicațiilor spyware şi a hackerilor. Dacă doriți activarea Windows Firewall şi a Windows Defender (doar pe Windows Vista) după dezinstalarea BitDefender, selectați căsuțele corespunzătoare.

  Faceți clic pe **Dezinstalare** pentru a iniția ştergerea completă a BitDefender Total Security 2009 de pe calculatorul dumneavoastră.

  În timpul procesului de dezinstalare, vi se va cere să ne trimiteți comentariile şi sugestiile dumneavoastră legate de BitDefender. Faceți clic pe **OK** pentru a răspunde unui chestionar online constând în cel mult cinci întrebări scurte. Dacă nu doriți să completați chestionarul, faceți clic pe **Anulare**.

  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 ştergeţi subdirectorul `BitDefender` din directorul `Program Files`.

A apărut o eroare în timpul dezinstalării BitDefender

Dacă în timpul dezinstalării BitDefender apare o eroare, procesul de dezinstalare este oprit şi va apărea o nouă fereastră. Faceți clic pe **Dezinstalare** pentru a vă asigura că BitDefender a fost dezinstalat complet. Utilitarul de dezinstalare va şterge toate fişierele şi cheile din regiştri care nu au fost şterse în timpul procesului automatizat de dezinstalare.

Administrare elementară

4. Introducere

O dată ce ați instalat BitDefender, calculatorul dumneavoastră este protejat.

4.1. Porniți BitDefender Total Security 2009

Primul pas în obținerea celor mai bune rezultate de la BitDefender este de a porni aplicația.

Pentru a accesa interfața principală a BitDefender Total Security 2009, utilizați meniul Start al Windows, urmând calea **Start** → **Programe** → **BitDefender 2009** → **BitDefender Total Security 2009** sau, mai rapid, faceți dublu-clic pe **iconița BitDefender** din bara de sistem.

4.2. Modul de vizualizarea a interfeței cu utilizatorul

BitDefender Total Security 2009 îndeplineşte deopotrivă cerințele persoanelor foarte tehnice şi pe cele ale începătorilor în utilizarea calculatorului. Aşadar, interfața grafică este proiectată pentru a se potrivi fiecărei categorii de utilizatori.

Puteți alege modul de vizualizare de bază sau pe cel avansat în funcție de experiența cu produsul nostru.

Notă
Puteți selecta cu uşurință una dintre aceste ferestre făcând clic, respectiv, pe butonul **Comută pe Elementar** sau butonul **Comută pe Avansat**.

4.2.1. Modul de bază

Modul Elementar este o interfață simplă care oferă acces la toate modulele la un nivel elementar. Va trebui să urmăriți avertismentele şi alertele critice şi să rezolvați problemele nedorite.

Modul de bază

- După cum se poate observa, în partea de sus a ferestrei există două butoane si o bara de stare.

Element	*Descriere*
Setări	Deschide o fereastră unde puteți activa sau dezactiva cu uşurință module importante de securitate (Firewall, modul ascuns, actualizarea automată, modul pentru jocuri, etc.).
Comută pe Avansat	Deschide fereastra modului Avansat. Aici puteți vedea lista completă a modulelor şi puteți configura în detaliu fiecare componentă. BitDefender va reține această opțiune data viitoare când veți deschide interfața cu utilizatorul.
Status	Conține informații despre şi vă ajută să remediați vulnerabilitățile care pot afecta securitatea calculatorului dumneavoastră.

- În partea de mijloc a ferestrei sunt disponibile cinci taburi.

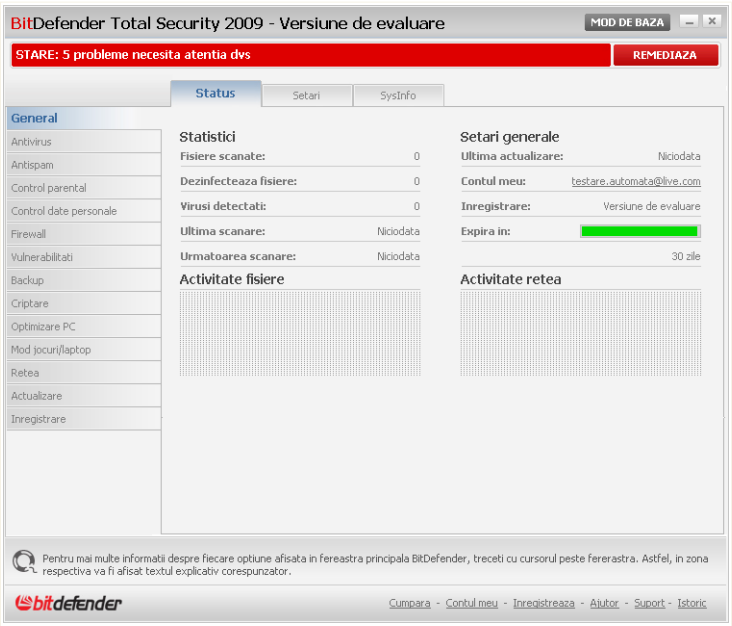
Tab	Descriere
Sumar	Afişează statistici importante despre produs şi statusul înregistrării, împreună cu linkuri către cele mai importante sarcini la cerere.
Securitate	Afişează starea modulelor de securitate (antivirus, antiphishing, firewall, antispam, criptare mesagerie instant, confidenţialitate, verificare vulnerabilităţi şi actualizare) şi linkuri către sarcini de verificare antivirus, actualizări şi vulnerabilităţi.
Optimizare	Afişează starea caracteristicilor BitDefender menite a optimiza performanţele sistemului dumneavoastră şi linkuri către sarcinile de optimizare.
Administrare fişiere	Afişează starea seifului de fişiere şi a modulelor de backup şi linkuri către sarcinile seifului de fişiere şi către sarcinile de backup.
Reţea	Afişează structura reţelei BitDefender.

- În plus, fereastră BitDefender conţine mai multe linkuri utile.

Link	Descriere
Contul meu	Vă permite să creaţi sau să vă conectaţi la contul dumneavoastră BitDefender. Contul BitDefender vă oferă acces gratuit la suport tehnic.
Înregistrează	Vă permite să introduceţi o nouă serie de înregistrare sau să vedeţi seria curentă de înregistrare şi starea înregistrării.
Ajutor	Deschide un fişier de ajutor care vă ajută să utilizaţi BitDefender.
Suport	Vă permite să contactaţi echipa de suport a BitDefender.
Istoric	Vă permite să vedeţi un istoric detaliat al tuturor sarcinilor efectuate de BitDefender pe sistemul dumneavoastră.

4.2.2. Modul avansat

Modul Avansat oferă acces la fiecare componenta a produsului BitDefender. Puteți configura setările avansate şi urmări caracteristicile avansate.



Modul avansat

- După cum se poate observa, în partea de sus a ferestrei există un buton si o bara de stare.

Element	Descriere
Comută pe Elementar	Deschide fereastra modului de bază. Aici puteți vedea interfața de bază a BitDefender care include principalele module (Securitate, Optimizare, Gestiune fişiere, Rețea) şi o pagină de gardă. BitDefender va reține această opțiune data viitoare când veți deschide interfața cu utilizatorul.

Element	Descriere
Status	Conține informații despre şi vă ajută să remediați vulnerabilitățile care pot afecta securitatea calculatorului dumneavoastră.

- În partea stângă a ferestrei există un meniu care conține toate modulele de securitate.

Modul	Descriere
General	Vă permite să accesați setările generale sau să vizualizați pagina de gardă şi informații detaliate despre sistem.
Antivirus	Vă permite să configurați scutul antivirus şi operațiile de scanare în detaliu, să setați excepții şi să configurați modulul de carantină.
Antispam	Vă permite să țineți la distanță mesajele spam de căsuța dumneavoastră de mesaje şi să configurați setările Antispam în detaliu.
Firewall	Vă protejează calculatorul de tentative de conexiune neautorizată la ieşire sau la intrare. Modulul este asemănător unui paznic – supraveghează conexiunea la Internet şi monitorizează aplicațiile cărora le este permis accesul la Internet precum şi pe cele care trebuie blocate.
Control date	Vă permite să preveniți furtul de date de pe calculatorul dumneavoastră şi să vă protejați confidențialitatea în timp ce sunteți online.
Control parental	Vă permite să vă protejați copiii împotriva conținutului inadecvat utilizând regulile dumneavoastră privind accesul la calculator.
Sarcini de backup	Vă permite să creați copii de siguranță ale datelor dumneavoastră pe calculator, pe discuri amovibile sau pe o locație din rețea pentru a le putea restaura atunci când este nevoie.
Criptare	Vă permite să criptați comunicațiile prin Yahoo şi Windows Live (MSN) Messenger şi să criptați local fişierele, directoarele sau partițiile.

Modul	Descriere
Vulnerabilitate	Vă permite să mențineți actualizate cele mai importante aplicații de pe calculatorul dumneavoastră.
Optimizare	Vă permite să îmbunătățiți performanțele calculatorului dumneavoastră defragmentând hard discul, curățând regiştrii, eliminând fişierele duplicate etc.
Modul pentru jocuri/laptop	Vă permite să amânați executarea sarcinilor BitDefender programate cât timp laptopul dumneavoastră funcționează pe baterii şi, de asemenea, să eliminați toate alertele şi pop-upurile atunci când vă jucați pe calculator.
Rețea	Vă permite să configurați şi să administrați mai multe calculatoare din locuința dumneavoastră.
Actualizare	Vă permite să obțineți informații despre cele mai recente actualizări, să actualizați produsul şi să configurați procesul de actualizare în detaliu.
Înregistrare	Vă permite să înregistrați BitDefender Total Security 2009, să schimbați seria de înregistrare sau să creați un cont BitDefender.

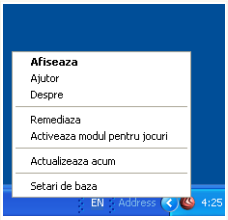
- În plus, fereastra BitDefender conține mai multe linkuri utile.

Link	Descriere
Contul meu	Vă permite să creați sau să vă conectați la contul dumneavoastră BitDefender. Contul BitDefender vă oferă acces gratuit la suport tehnic.
Înregistrează	Vă permite să introduceți o nouă serie de înregistrare sau să vedeți seria curentă de înregistrare şi starea înregistrării.
Ajutor	Deschide un fişier de ajutor care vă ajută să utilizați BitDefender.
Suport	Vă permite să contactați echipa de suport a BitDefender.
Istoric	Vă permite să vedeți un istoric detaliat al tuturor sarcinilor efectuate de BitDefender pe sistemul dumneavoastră.

4.3. Iconița BitDefender din bara de sistem

Pentru o administrare mai rapidă a produsului, puteți folosi şi iconița BitDefender din bara de sistem.

Dacă faceți dublu-clic pe această iconiță, se va deschide interfața BitDefender. De asemenea, făcând clic-dreapta pe iconiță, un meniu contextual vă va oferi posibilitatea unei administrări rapide a BitDefender.



Iconița BitDefender

- **Afişează** - deschide interfața BitDefender.
- **Ajutor** - deschide documentația electronică care explică în detaliu produsul BitDefender Total Security 2009.
- **Despre** - deschide pagina web a BitDefender.
- **Repară toate problemele** - vă ajută să remediați problemele ce afecteaza securitatea sistemului.
- **Activează / Deactivează modul pentru jocuri** - activează / deactivează modul pentru jocuri.
- **Actualizează acum** - inițiază o actualizare imediată. Va apărea o nouă fereastră în care puteți vedea starea actualizării.
- **Setări de bază** - vă permite să activați sau să dezactivați cu uşurință module importante de securitate. Va apărea o nouă fereastră de unde le puteți activa / dezactiva cu un singur clic.

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

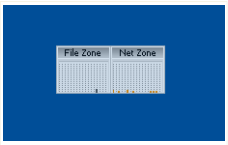
Dacă există probleme critice care afectează securitatea sistemului dumneavoastră, un semn de exclamare este afişat pe iconița BitDefender. Puteți ține cursorul mouse-ului deasupra iconiței pentru a vedea numărul problemelor care afectează securitatea sistemului.

4.4. Bara de scanare

Bara de scanare este o reprezentare grafică a activității de scanare din sistemul dumneavoastră.

Barele gri (zona **Fişiere**) reprezintă numărul de fişiere scanate pe secundă, pe o scară de la 0 la 50.

Barele portocalii din zona **Internet** reprezintă numărul de kiloocteți transferați (trimişi şi 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 afişarea unui X roşu deasupra zonei corespunzătoare (**Fişiere** sau **Internet**).

Puteți utiliza **Bara de scanare** pentru a scana obiecte. În acest scop, trageți obiectele care doriți să fie scanate peste ea. Pentru mai multe informații, consultați "*Scanare prin drag&drop*" (p. 202).

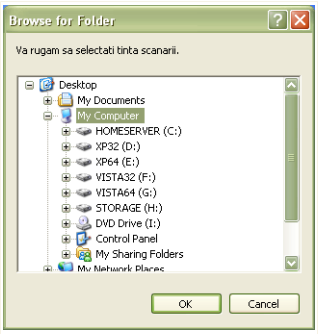
Când nu mai doriți să vedeți reprezentarea grafică, faceți doar clic-dreapta pe ea şi selectați **Închide**. Pentru a ascunde permanent această fereastră, urmați aceşti paşi:

1. Faceți clic pe **Mod avansat** (dacă sunteți în **modul de bază**).
2. Faceți clic pe **General** în meniul din stânga.
3. Faceți clic pe tabul **Setări**.
4. Debifați căsuța **Afişează bara de scanare (graficul de pe ecran al activității produsului)**.

4.5. Scanare manuală BitDefender

Dacă doriți să scanați rapid un anumit fişier, puteți utiliza scanarea manuală BitDefender.

Pentru a accesa programul asistent de scanare manuală, utilizați meniul Windows Start, urmând calea **Start → Programe → BitDefender 2009 → Scanare manuală BitDefender**. Va apărea următoarea fereastră:



Scanare manuală BitDefender

Tot ce trebuie să faceți este să căutați în listă directorul care doriți să fie scanat, să îl selectați şi să faceți clic pe **OK**. Va apărea programul asistent de scanare care vă va ghida de-a lungul procesului de scanare.

4.6. Modul pentru jocuri

Modul pentru jocuri modifică temporar setările de protecție 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 şi consumul de memorie.
- Se amână actualizările şi scanările automate.
- Se elimină toate alertele şi pop-upurile.
- Se scanează doar cele mai importante fişiere.

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

4.6.1. Utilizarea modului pentru jocuri

Pentru a activa modul pentru jocuri, utilizați una dintre următoarele metode:

- Faceți clic-dreapta pe icoana BitDefender din bara de sistem şi 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 aceleaşi metode ca şi la activarea sa.

4.6.2. Schimbarea combinației de taste

Pentru a schimba combinația de taste, urmați aceşti paşi:

1. Faceți clic pe **Mod avansat** (dacă sunteți în **modul de bază**).
2. Faceți clic pe **Mod pentru jocuri/laptop** în meniul din stânga.
3. Faceți clic pe tabul **Mod pentru 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` şi `Alt` şi să tastați `D`.

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

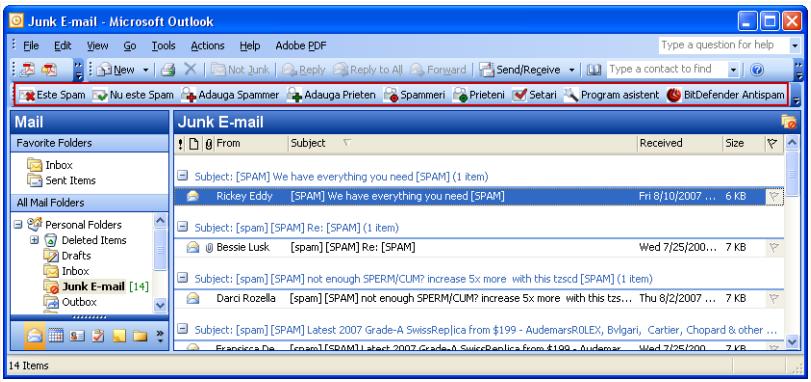
4.7. Integrarea cu clienții de mail

BitDefender se integrează direct, printr-o bară de comenzi intuitivă şi uşor de folosit, cu următorii clienți de mail:

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

4.7.1. Bara de comenzi BitDefender

În partea de sus a clientului dumneavoastră de mail, puteți vedea bara de comenzi Antispam.



Bara de comenzi BitDefender

Important
Diferența dintre BitDefender Antispam pentru Microsoft Outlook şi Outlook Express / Windows Mail este că mesajele SPAM sunt mutate în directorul **Spam** în Microsoft Outlook, în timp ce în Outlook Express / Windows Mail acestea sunt mutate în directorul **Deleted Items**. În ambele programe mesajelor li se adaugă cuvântul SPAM în subiect.

Directorul **Spam** este creat automat de BitDefender pentru Microsoft Outlook şi este listat la acelaşi nivel cu celelalte directoare din **Folder list** (Calendar, Contacts, etc).

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 şi 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 modulului Bayesian indicând că mesajul selectat nu este spam, iar BitDefender nu ar fi trebuit să îl marcheze. Mesajul va fi mutat din directorul **Spam** în directorul **Inbox**.

  Mesajele viitoare care seamănă cu acest mesaj 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 mesajului selectat la **lista de spammeri**.

Adaugă spamer

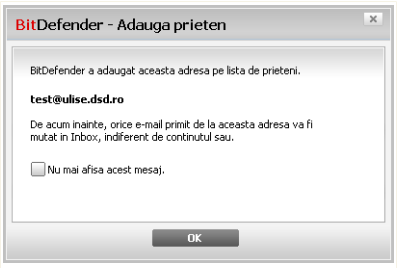
Selectați **Nu mai afişa acest mesaj** dacă nu doriți să vi se ceară confirmarea în momentul adăugării expeditorului la lista de prieteni.

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 mesajului selectat la **lista de prieteni**.



Adaugă prieten

Selectați **Nu mai afişa acest mesaj** dacă nu doriți să vi se ceară confirmarea în momentul adăugării expeditorului la 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 şterge intrări din **lista de spammeri** .

Dacă doriți să adăugați o adresă, selectați **E-mail** scrieți adresa şi faceți clic pe butonul . Adresa va apărea în **lista de spammeri**.

Important
Sintaxă: nume@domeniu.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:
- @domeniu.com, *domeniu.com and domeniu.com - toate mesajele primite de la domeniu.com vor fi etichetate ca SPAM;
- *domeniu* - toate mesajele primite de la domeniu(indiferent de sufixul domeniului) vor fi etichetate ca SPAM;
- *com - a- toate mesajele primite având sufixul domeniului com vor fi etichetate 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 şi faceți clic pe **Selectează**.

În ambele cazuri adresele de e-mail vor apărea în lista pentru importare. Selectați-le pe cele dorite şi faceți clic pe pentru a le adăuga la **lista de spammeri**. Dacă faceți clic pe toate adresele vor fi adăugate în listă.

Pentru a şterge un obiect din listă, selectați-l şi faceți clic pe butonul **Şterge**. Dacă faceți clic pe butonul **Şterge listă** veți şterge toate intrările din listă, dar atenție: este imposibil să le recuperați.

Folosiți butoanele **Salvare**/ **Încărcare** pentru a salva/încărca **lista de spammeri** într-o anumită locație. Fişierul va avea extensia `.bwl`.

Pentru a reseta conținutul listei curente atunci când încărcați o listă salvată anterior selectați **Goleşte lista la încărcare**.

Faceți clic pe **Salvare** şi **OK** pentru a salva modificările şi 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 şterge intrări din **lista de prieteni**.

Dacă doriți să adăugați o adresă, selectați opțiunea **E-mail**, scrieți adresa şi faceți clic pe butonul ⊠. Adresa va apărea în **lista de prieteni**.

Important
Sintaxă: nume@domeniu.com.

Dacă doriți să adăugați un domeniu, selectați **Domeniul**, scrieți numele domeniului şi faceți clic pe butonul ⊠. Domeniul va apărea în **lista de prieteni**.

Important
Sintaxă:

- @domeniu.com, *domeniu.com şi domeniu.com - toate mesajele primite de la domeniu.com vor ajunge în directorul **Inbox** indiferent de conținut;
- *domeniu* - toate mesajele primite de la domeniu (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 adaugați la **lista de prieteni**. Alegeți adresele dorite şi faceți clic pe **Selectează**.

În ambele cazuri adresele de e-mail vor apărea în lista pentru importare. Selectați-le pe cele dorite şi faceți clic pe pentru a le adăuga la **lista de prieteni**. Dacă faceți clic pe toate adresele vor fi adăugate în listă.

Pentru a şterge un obiect din listă, selectați-l şi faceți clic pe butonul **Şterge**. Dacă faceți clic pe butonul **Şterge listă** veți şterge toate intrările din listă, dar atenție: este imposibil să le recuperați.

Folosiți butoanele **Salvare**/ **Încărcare** pentru a salva/încărca **lista de prieteni** într-o anume locație. Fişierul va avea extensia `.bwl`.

Pentru a reseta conținutul listei curente atunci când încărcați o listă salvată anterior selectați **Goleşte lista la încărcare**.

Notă

Vă recomandăm să adăugați numele şi adresele prietenilor în **lista de prieteni**. BitDefender nu va bloca mesajele de la cei de pe listă; de aceea, adăugarea prietenilor în listă vă asigură că mesajele legitime vor ajunge în Inbox.

Faceți clic pe **Salvare** şi **OK** pentru a salva modificările şi 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 ştergeţi baza de date a filtrului şi să reeducaţi Filtrul Bayesian. Faceţi clic pe **Şterge baza de date antispam** pentru a reseta baza de date Bayesiană.

Utilizaţi butoanele **Salvează baza de date Bayesiană**/ **Încarcă baza de date Bayesiană** pentru a salva /încărca baza de date Bayesiană într-o/ dintr-o anumită locaţie. Fişierul va avea extensia `.dat`.

Faceţi clic pe tabul **Alerte** dacă doriţi să accesaţi secţiunea în care puteţi dezactiva apariţia ferestrelor de confirmare pentru butoanele **Adaugă spammer** şi **Adaugă prieten**.

Notă

În fereastra **Alerte** puteţi de asemenea să activaţi/dezactivaţi apariţia alertei **Selectaţi un mesaj email**. Această alertă apare atunci când selectaţi un grup în loc de un mesaj email.

- **Asistent** - deschide programul asistent care vă va ghida prin procesul de educare a motorului de învățare (bayesian), proces ce va creşte eficiența filtrului Antispam. De asemenea, puteți adăuga adrese din **Address Book** la **lista de prieteni** / **lista de spammeri**.
- **BitDefender Antispam** - deschide interfața BitDefender.

4.7.2. 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 şi lista de spammeri şi să educați motorul de învățare (bayesian) pentru a creşte eficiența filtrelor Antispam.

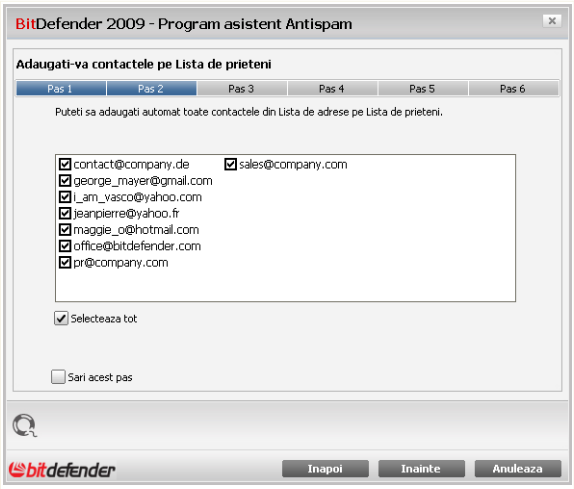
Notă
Programul asistent mai poate fi lansat, oricând doriți, făcând clic pe butonul **Asistent** din bara de comenzi Antispam.

Pasul 1/6 - Fereastră de întâmpinare

Fereastra de întâmpinare

Faceți clic pe **Înainte**.

Pasul 2/6 - Completați lista de prieteni



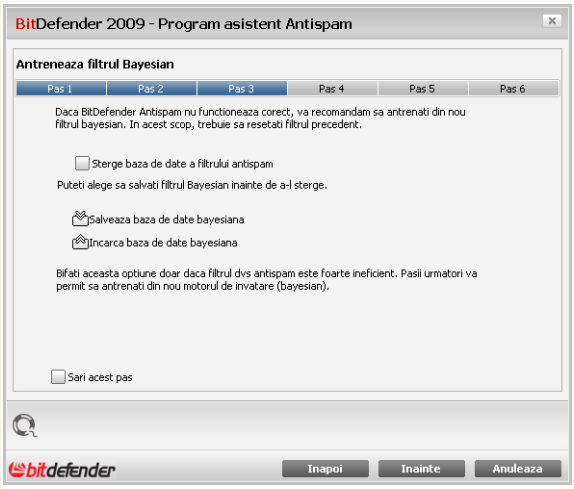
Completați lista de prieteni

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 la lista de prieteni, bifați **Selectează tot**.

Faceți clic pe **Sări acest pas** dacă doriți să săriți acest pas. Faceți clic pe **Înapoi** pentru a reveni la pasul anterior sau pe **Înainte** pentru a trece la pasul următor.

Pasul 3/6 - Șterge baza de date Bayesiană



Șterge baza de date Bayesiană

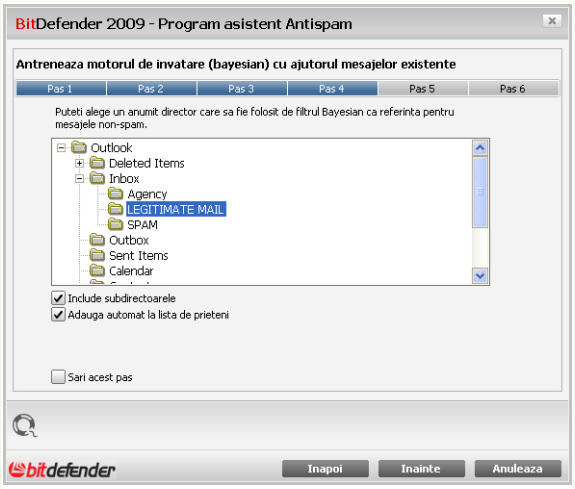
Există posibilitatea să descoperiți că filtrul Antispam a început să-şi piardă eficiența. Aceasta se poate întâmpla din cauza educării incorecte (ați etichetat din greşeală unele mesaje legitime ca Spam, sau invers). Dacă filtrul este ineficient, trebuie să ştergeți baza de date a filtrului şi să reeducați filtrul urmând paşii acestui program asistent.

Selectați **Şterge baza de date a filtrului antispam** dacă doriți să ştergeți baza de date a Filtrului Bayesian.

Utilizați butoanele **Salvează baza de date Bayesiană**/ **Încarcă baza de date Bayesiană** pentru a salva /încărca Baza de date Bayesiană într-o/ dintr-o anumită locație. Fişierul va avea extensia `.dat`.

Faceți clic pe **Sări acest pas** dacă doriți să săriți acest pas. Faceți clic pe **Înapoi** pentru a reveni la pasul anterior sau pe **Înainte** pentru a trece la pasul următor.

Pasul 4/6 - Educați filtrul Bayesian cu mesaje legitime



Educați filtrul Bayesian cu mesaje legitime

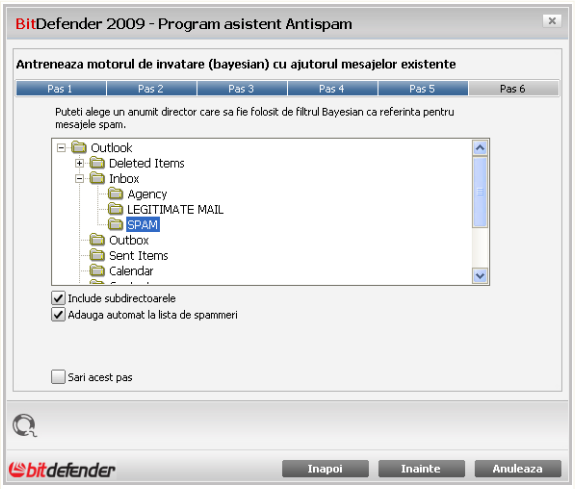
Selectați un director care conține mesaje e-mail legitime. Aceste mesaje vor fi folosite pentru a educa filtrul Antispam.

Sub lista de directoare se găsesc două opțiuni avansate:

- **Include subdirectoarele** - pentru a include subdirectoarele în selecție.
- **Adaugă automat la lista de prieteni** - pentru a adăuga expeditorii în **lista de prieteni**.

Faceți clic pe **Sări acest pas** dacă doriți să săriți acest pas. Faceți clic pe **Înapoi** pentru a reveni la pasul anterior sau pe **Înainte** pentru a trece la pasul următor.

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.

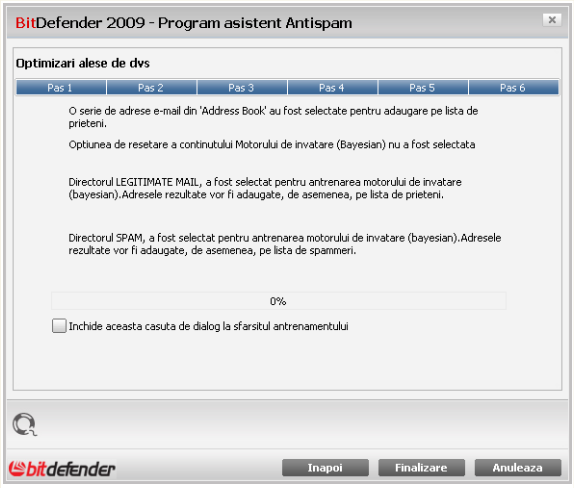
Important
Directorul nu trebuie să conțină niciun mesaj legitim, altfel performanțele filtrului Antispam vor fi considerabil reduse.

Sub lista de directoare se găsesc două opțiuni avansate:

- **Include subdirectoarele** - pentru a include subdirectoarele în selecție.
- **Adaugă automat la lista de spammeri** - pentru a adăuga expeditorii în **lista de spammeri**.

Faceți clic pe **Sări acest pas** dacă doriți să săriți acest pas. Faceți clic pe **Înapoi** pentru a reveni la pasul anterior sau pe **Înainte** pentru a trece la pasul următor.

Step 6/6 - Sumar



Rezumat

În această fereastră puteți vedea toate setările făcute în programul asistent. Puteți face orice schimbări, revenind la paşii anteriori (faceți clic pe **Înapoi**).

Dacă nu doriți să faceți nicio modificare, faceți clic pe **Finalizare** pentru a închide programul asistent.

4.8. Integrarea cu browserele web

BitDefender vă protejează împotriva tentativelor de phishing atunci când navigați pe Internet. Acesta scanează paginile web accesate şi vă alertează dacă sunt amenințări phishing. O listă albă de pagini web care nu vor fi scanate de BitDefender poate fi configurată.

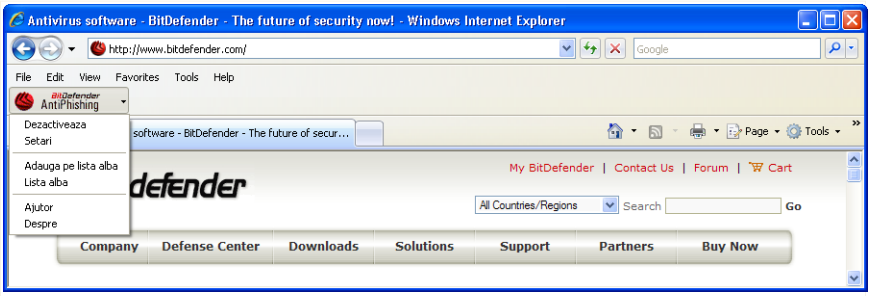
BitDefender se integrează direct, printr-o bară de comenzi intuitivă şi uşor de folosit, cu următoarele browsere web:

- Internet Explorer
- Mozilla Firefox

Puteți administra uşor şi eficient protecția antiphishing şi lista albă utilizând bara de comenzi BitDefender Antiphishing integrată în browserele web de mai sus.

Bara de comenzi antiphishing, reprezentată prin **iconița BitDefender**, este situată în partea superioară 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** şi bifați **BitDefender Toolbar**.



Bara de comenzi antiphishing

Următoarele comenzi sunt disponibile pe meniul barei de instrumente:

- **Activează / Dezactivează** - activează / dezactivează bara de comenzi antiphishing a BitDefender.

  Notă
  Dacă alegeți să dezactivați bara de comenzi antiphishing, nu veți mai fi protejat împotriva tentativelor de phishing.

- **Setări** - deschide o fereastră în care puteți specifica setările barei de comenzi antiphishing.

  Următoarele opțiuni sunt disponibile:
  - **Activează scanarea** - activează scanarea antiphishing.
  - **Întreabă înainte de a adăuga în lista albă** - vă avertizează înainte de a adăuga o pagină web în lista albă.
- **Adaugă la 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.

- **Vizualizează lista albă** - deschide lista albă.

  Puteți vedea lista tuturor paginilor web care nu sunt verificate de motoarele antiphishing ale BitDefender.

  Dacă doriți să ştergeți 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 **Şterge** corespunzător paginii.

  Puteți adăuga paginile web în care aveți deplină încredere la lista albă pentru a nu mai fi scanate de motoarele antiphishing. Pentru a adăuga o pagină web la lista albă, introduceți adresa acesteia în câmpul corespunzător şi faceți clic pe **Adaugă**.
- **Ajutor** - deschide documentația electronică.
- **Despre** - deschide o fereastră în care puteți vedea informații despre BitDefender şi unde să apelați pentru ajutor în cazul unei probleme.

4.9. Integrarea cu clienții de mesagerie instant

BitDefender oferă capabilități de criptare pentru a vă proteja documentele confidențiale şi conversațiile dumneavoastră prin mesageria instant, prin Yahoo Messenger şi MSN Messenger.

În mod implicit, BitDefender criptează toate sesiunile dumneavoastră de chat prin mesagerie instant cu condiția ca:

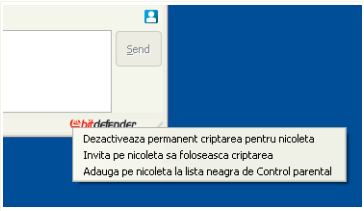
- Partenerul dumneavoastră de chat are instalată o versiune de BitDefender care suportă criptarea mesageriei instant (IM), iar Criptarea IM este activată pentru aplicația de mesagerie instant folosită pentru chat.
- Atât dumneavoastră, cât si partenerul dumneavoastră de chat, să utilizați fie Yahoo Messenger, fie Windows Live (MSN) Messenger.

Important
BitDefender nu va cripta o conversație dacă un partener de chat foloseste o aplicație web pentru chat, cum ar fi Meebo, sau alte aplicații de chat care suportă Yahoo Messenger sau MSN.

Puteți configura uşor criptarea mesageriei instant folosind bara de comenzi BitDefender din fereastra de chat.

Făcând clic-dreapta pe bara de comenzi BitDefender, veți avea următoarele opțiuni:

- Activarea / Dezactivarea permanentă a criptării pentru un anumit partener de chat
- Invitarea unui anumit partener de chat pentru a utiliza criptarea
- Înlăturarea unui anumit partener de chat de pe lista neagră a Controlului parental



Opțiuni criptare mesagerie instant

Trebuie doar să faceți clic pe una dintre opțiunile menționate mai sus pentru a o utiliza.

5. Pagina de gardă

Făcând clic pe tabul Pagina de gardă vă vor fi furnizate statistici importante despre produs şi starea înregistrării, împreună cu linkuri către cele mai importante sarcini la cerere.

Pagina de gardă

Pagina de gardă conține mai multe secțiuni:

- **Statistici** - Afişează informații importante referitoare la activitatea BitDefender.
- **Prezentare generală** - Afişează informații referitoare la actualizare, contul dumneavoastră, înregistrare şi licență.
- **Zonă fişiere** - Indică evolutia numărului de obiecte scanate de către BitDefender Antimalware. Înălțimea barelor indică intensitatea traficului în intervalul de timp respectiv.
- **Zonă rețea** - Indică evolutia traficului de rețea filtrat de către firewallul BitDefender. Înălțimea barelor indică intensitatea traficului în intervalul de timp respectiv.

- **Sarcini** - Oferă linkuri către cele mai importante sarcini de securitate: scanare completă sistem, scanare profundă, actualizare imediată.

5.1. Statistici

Dacă doriți să urmăriți activitatea BitDefender, puteți începe cu secțiunea Statistici.

Element	*Descriere*
Fişiere scanate	Indică numărul de fişiere care au fost verificate după malware la ultima scanare.
Fişiere dezinfectate	Indică numărul de fişiere care au fost dezinfectate la ultima scanare.
Viruşi detectați	Indică numărul viruşilor detectați în sistemul dumneavoastră la ultima scanare.
Scanări de porturi blocate	Indică numărul de scanări de porturi blocate de firewallul 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. Mențineți firewallul şi modul ascuns activate pentru a fi protejat împotriva scanărilor de porturi.
Sarcini de backup finalizate	Arată de câte ori ați făcut copii de siguranță ale fişierelor dumneavoastră.

5.2. Descriere generală

Aici puteti vedea un sumar al statisticilor cu privire la actualizare, contul dumneavoastră, înregistrare şi licență.

Element	*Descriere*
Ultima actualizare	Indică data la care produsul dumneavoastră BitDefender a fost actualizat ultima oară. Vă rugăm să efectuați actualizări în mod regulat, pentru a avea un sistem complet protejat.
Contul meu	Indică adresa de e-mail pe care o puteți utiliza pentru a vă accesa contul online, unde vă puteți recupera seria de înregistrare pierdută şi puteți beneficia de suport BitDefender si alte servicii personalizate.

Element	Descriere
Înregistrare	Indică tipul şi 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.

Pentru a actualiza BitDefender, faceți clic pe butonul **Actualizează acum** din secțiunea de sarcini.

Pentru a crea sau a vă conecta la contul dumneavoastră BitDefender, urmați aceşti paşi:

1. Faceți clic pe linkul **Contul meu** situat în partea de jos a ferestrei. Se va deschide o pagina web.
2. Introduceți numele dumneavoastră de utilizator şi parola şi faceți clic pe butonul **Login**.
3. Pentru a crea un cont BitDefender, selectați **You don't have an account?** şi furnizați informațiile solicitate.

Notă
Informațiile furnizate aici vor rămâne confidențiale.

Pentru a înregistra BitDefender Total Security 2009, urmați aceşti paşi:

1. Faceți clic pe linkul **Contul meu** situat în partea de jos a ferestrei. Va apărea un program asistent de înregistrare.
2. Faceți clic pe butonul **Doresc să înregistrez produsul cu o noua serie**.
3. Introduceți noua serie de înregistrare în câmpul corespunzător.
4. Faceți clic pe **Finalizare**.

Pentru a cumpara o nouă serie de înregistrare, urmați aceşti paşi:

1. Faceți clic pe linkul **Contul meu** situat în partea de jos a ferestrei. Va apărea un program asistent de înregistrare.
2. Faceți clic pe **Reînnoire serie de înregistrare BitDefender**. Se va deschide o pagină web.
3. Faceți clic pe butonul **Cumpără acum**.

5.3. Sarcini

Aici puteți găsi linkuri către cele mai importante sarcini de securitate: scanare completă sistem, scanare profundă, actualizare imediată.

Următoarele butoane sunt disponibile:

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

5.3.1. Scanarea cu BitDefender

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

Sarcina	Descriere
Scanare completă sistem	Scanează întregul sistem, cu excepția arhivelor. În configurația implicită, se scanează după toate tipurile de aplicații malițioase care amenință securitatea sistemului dumneavoastră, cum ar fi viruşii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) şi altele.
Scanare profundă	Scanează întregul sistem. În configurația implicită, se scanează după toate tipurile de aplicații malițioase care amenință securitatea sistemului dumneavoastră, cum ar fi viruşii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) şi altele.

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

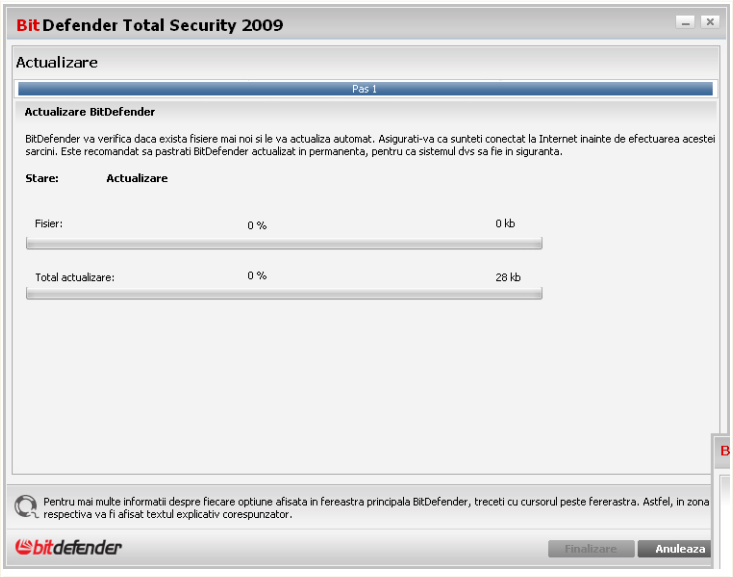
Atunci când inițiați un proces de scanare la cerere, fie o scanare rapidă sau completă a sistemului, va apărea programul asistent de scanare.

Urmați programul asistent în trei paşi pentru a realiza procesul de scanare.

5.3.2. Actualizarea BitDefender

În fiecare zi sunt descoperite şi 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 şi 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 şi 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 şi, în acelaşi timp, orice vulnerabilitate va fi exclusă.

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

Notã
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.

6. Securitate

BitDefender conține un modul de securitate care vă ajută să îl actualizați şi să vă protejați sistemul de viruşi.

Pentru a accesa modulul de securitate, faceți clic pe tabul **Securitate**.

Securitate

Modulul Securitate conține două secțiuni:

- **Componente monitorizate** - Vă permite să vedeți lista completă a componentelor monitorizate pentru fiecare modul de securitate. Puteți alege care dintre module să fie monitorizate. Este recomandată monitorizarea tuturor componentelor.
- **Sarcini** - Aici puteți găsi linkuri către cele mai importante sarcini de securitate: scanare completă sistem, scanare profundă, actualizare imediată.

6.1. Componente monitorizate

Componentele monitorizate sunt grupate în mai multe categorii.

Categorie	Descriere
Securitate locală	Aici puteți verifica starea fiecărui modul de securitate care protejează obiectele stocate pe calculatorul dumneavoastră (fişiere, regiştri, memorie, etc.)
Securitate online	Aici puteti verifica starea modulelor de securitate care vă protejează tranzacțiile online şi calculatorul când sunteți conectat la Internet.
Securitate rețea	Aici puteți verifica starea modulului Firewall care vă protejează împotriva hackerilor.
Control parental	Aici puteti verifica starea Controlului parental care vă permite să restricționați accesul copiilor dumneavoastră la Internet şi la anumite aplicații.
Căutare vulnerabilități	Aici puteți verifica dacă aplicații critice de pe calculatorul dumneavoastră sunt la zi. Parolele conturilor Windows sunt verificate pe baza unor reguli de securitate.

Faceți clic pe semnul “+” pentru a deschide o categorie sau pe “-” pentru a închide categoria.

6.1.1. Securitate locală

Ştim că este important să fiți înştiințat ori de câte ori o problemă poate afecta securitatea calculatorului dumneavoastră. Prin monitorizarea fiecărui modul de securitate, BitDefender Total Security 2009 vă va înştiința nu numai atunci când configurați setări care ar putea afecta securitatea calculatorului dumneavoastră, ci şi atunci când uitați să executați sarcini importante.

Problemele privind securitatea locală sunt descrise în propoziții explicite. Dacă există probleme care ar putea afecta securitatea calculatorului dumneavoastră, veți vedea un buton roşu **Repară** în dreptul fiecăreia dintre acestea. Altfel, este afişat un buton verde **OK**.

Problemă	Descriere
Protecția în timp real este activată	Asigură scanarea tuturor fişierelor accesate de către dumneavoastră sau de către o aplicație care rulează pe acest sistem.

Problemă	Descriere
Ați scanat calculatorul după malware astăzi	Este recomandat să executați o scanare la cerere, cât mai curând posibil, pentru a verifica dacă fișierele stocate pe calculatorul dumneavoastră conțin malware.
Actualizarea automată este activată	Vă rugăm să mențineți activată actualizarea automată pentru a vă asigura că semnăturile de malware ale produsului dumneavoastră BitDefender sunt actualizate în mod regulat.
Actualizare în curs	Actualizarea produsului şi a semnăturilor de malware este în curs de desfăşurare.

Atunci când butoanele de stare au culoarea verde, sistemul dumneavoastră este în siguranță. Pentru a remedia potențialele probleme, urmați aceşti paşi:

1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

Dacă nu doriți ca o anumită problemă să fie monitorizată, debifați căsuța **Da, monitorizează această componentă**.

6.1.2. Securitate online

Problemele privind securitatea online sunt descrise în propoziții explicite. Dacă există probleme care ar putea afecta securitatea calculatorului dumneavoastră, veți vedea un buton roşu **Repară** în dreptul fiecăreia dintre acestea. Altfel, este afişat un buton verde **OK**.

Problemă	Descriere
Protecția în timp real pentru traficul web (HTTP) este activată	Este recomandat să mențineți protecția web (HTTP) activată pentru a vă proteja calculatorul împotriva aplicațiilor malițioase care se răspândesc prin intermediul site-urilor web şi împotriva fişierelor infectate descărcate.
Protecția în timp real pentru e-mailuri este activată	Protecția pentru traficul e-mail asigură că e-mailurile dumneavoastră sunt filtrate după malware şi conținut spam.

Problemă	Descriere
Protecția în timp real pentru traficul IM este activată	Este recomandat să activați protecția completă pentru traficul de mesagerie instant pentru a asigura securitatea calculatorului dumneavoastră.
Controlul identității este activat	Vă ajută să păstrați datele confidențiale în siguranță scanând tot traficul web şi mail după anumite stringuri. Este recomandat să activați Controlul identității pentru a împiedica furtul datelor dumneavoastră confidențiale (adresa de mail, parole, numere de carduri de credit etc).
Criptarea conversațiilor prin IM este activată	În cazul în care contactele dumneavoastră de IM au BitDefender 2009 instalat, toate conversațiile IM prin Yahoo! Messenger şi Windows Live Messenger vor fi criptate. Este recomandat să aveți activată criptarea IM pentru a vă asigura că discuțiile dumneavoastră prin mesageria instant rămân private.
Protecția antiphishing pentru Firefox este activată	BitDefender vă protejează împotriva tentativelor de phishing atunci când navigați pe Internet.
Protecția antiphishing pentru Internet Explorer este activată	BitDefender vă protejează împotriva tentativelor de phishing atunci când navigați pe Internet.

Atunci când butoanele de stare au culoarea verde, sistemul dumneavoastră este în siguranță. Pentru a remedia potențialele probleme, urmați aceşti paşi:

1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

Dacă nu doriți ca o anumită problemă să fie monitorizată, debifați căsuța **Da, monitorizează această componentă**.

6.1.3. Securitate rețea

Atunci când calculatorul dumneavoastră face parte dintr-o rețea, doriți cu siguranță ca acesta să fie protejat împotriva hackerilor şi să fie blocate orice conexiuni neautorizate.

Problemele privind securitatea rețelei sunt descrise în propoziții explicite. Dacă există probleme care ar putea afecta securitatea calculatorului dumneavoastră, veți vedea un buton roşu **Repară** în dreptul fiecăreia dintre acestea. Altfel, este afişat un buton verde **OK**.

Problemă	*Descriere*
Firewallul este activat	Vă protejează calculatorul de atacurile din exterior ale hackerilor şi aplicațiilor periculoase.

Atunci când butoanele de stare au culoarea verde, sistemul dumneavoastră este în siguranță. Pentru a remedia potențialele probleme, urmați aceşti paşi:

1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

Dacă nu doriți ca o anumită problemă să fie monitorizată, debifați căsuța **Da, monitorizează această componentă**.

6.1.4. Control parental

Controlul parental monitorizează starea modulelor care vă permit să restricționați accesul copiilor dumneavoastră la Internet şi la anumite aplicații.

Problemele privind modulul de control parental sunt descrise în propoziții explicite. Dacă există ceva care ar putea afecta copiii dumneavoastră, veți vedea un buton roşu **Repară** în dreptul fiecărei probleme. Altfel, este afişat un buton verde **OK**.

Problemă	*Descriere*
Controlul parental nu este configurat	Modulul Control parental poate bloca accesul la pagini web cu conținut inadecvat, poate bloca accesul la Internet pentru anumite perioade şi poate filtra traficul mail, IM şi web după anumite cuvinte etc.

Atunci când butoanele de stare au culoarea verde, copiii dumneavoastră pot naviga în siguranță pe web. Pentru a remedia potențialele probleme, urmați aceşti paşi:

1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

Dacă nu doriți ca o anumită problemă să fie monitorizată, debifați căsuța **Da, monitorizează această componentă**.

6.1.5. Căutare vulnerabilități

Problemele privind vulnerabilitățile sistemului sunt descrise în propoziții explicite. Dacă există probleme care ar putea afecta securitatea calculatorului dumneavoastră, veți vedea un buton roşu **Repară** în dreptul fiecăreia dintre acestea. Altfel, este afişat un buton verde **OK**.

Problemă	*Descriere*
Căutarea de vulnerabilități este activată	Monitorizează sistemul de actualizare al Microsoft Windows şi al Microsoft Windows Office şi parolele conturilor Microsoft Windows pentru a vă asigura că sistemul dumneavoastră de operare este actualizat şi că parolele nu pot fi ghicite uşor.
Actualizări Microsoft critice	Instalează actualizările critice disponibile de la Microsoft.
Alte actualizări Microsoft	Instalează actualizările normale disponibile de la Microsoft.
Windows Automatic Updates este activat	Instalează noile actualizări de securitate pentru Windows imediat ce acestea sunt disponibile.
Administrator (parolă puternică)	Indică siguranța pe care o oferă parola configurată pentru un anumit utilizator (cât de uşor poate fi ghicită).

Atunci când butoanele de stare au culoarea verde, sistemul dumneavoastră este în siguranță. Pentru a remedia potențialele probleme, urmați aceşti paşi:

1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

Dacă nu doriți ca o anumită problemă să fie monitorizată, debifați căsuța **Da, monitorizează această componentă**.

6.2. Sarcini

Aici puteți găsi linkuri către cele mai importante sarcini de securitate: scanare completă sistem, scanare profundă, actualizare imediată.

Următoarele butoane sunt disponibile:

- **Scanare completă sistem** - inițiază o scanare completă a calculatorului dumneavoastră (arhivele nu sunt scanate).
- **Scanare completă sistem** - inițiază o scanare completă a calculatorului dumneavoastră (inclusiv arhivele).
- **Scanează Documentele mele** - inițiază o scanare rapidă a documentelor şi setărilor dumneavoastră.
- **Actualizează acum** - inițiază o actualizare imediată.
- **Verificare vulnerabilități**
- **Scanare personalizată**

6.2.1. Scanarea cu BitDefender

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

Sarcina	*Descriere*
Scanare completă sistem	Scanează întregul sistem, cu excepția arhivelor. În configurația implicită, se scanează după toate tipurile de aplicații malițioase care amenință securitatea sistemului dumneavoastră, cum ar fi viruşii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) şi altele.
Scanare profundă	Scanează întregul sistem. În configurația implicită, se scanează după toate tipurile de aplicații malițioase care amenință securitatea sistemului dumneavoastră, cum ar fi viruşii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) şi altele.
Scanează Documentele mele	Utilizați această sarcină pentru a scana directoare importante ale utilizatorului curent: `My Documents`, `Desktop` şi `StartUp`. Astfel, veți asigura siguranța

Sarcina	Descriere
	documentelor dumneavostră, un spațiu de lucru sigur şi rularea la pornirea sistemului a unor aplicații necompromise.
Scanare personalizată	Utilizați această sarcină pentru a selecta direct care fişiere şi directoare să fie scanate.

Notă

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

Atunci când inițiați un proces de scanare la cerere, fie o scanare rapidă sau completă a sistemului, va apărea programul asistent de scanare.

Urmați programul asistent în trei paşi pentru a realiza procesul de scanare.

Scanare personalizată

Făcând clic pe butonul **Scanare personalizată** şi urmând paşii programului asistent, puteți crea sarcini de scanare personalizate pe care, opțional, le puteți salva ca sarcini rapide.

Pasul 1/4 - Fereastra de întâmpinare

Aceasta este doar o pagină de bun venit.

Fereastra de întâmpinare

Cu ajutorul acestui program asistent vă veți putea scana calculatorul pentru a identifica eventualele pericole. Veți putea selecta anumite directoare şi/sau fişiere de scanat si veți putea stabili acțiuni de aplicat la detectarea unor fişiere infectate. De asemenea, veți primi un raport de scanare care vă va permite să evaluați nivelul de securitate al sistemului dumneavoastră. Parcurgeți fiecare pas şi configurați procesul de scanare după cum doriți.

Notă
Pentru a sări peste acest pas când veți mai utiliza acest program asistent, bifați căsuța corespunzătoare.

Faceți clic pe **Înainte** pentru a continua sau pe **Anulare** dacă doriți să părăsiți programul asistent.

Pasul 2/4 - Selectați obiectele de scanat

Aici puteți specifica care fişiere şi directoare să fie scanate.

Selectați obiectele de scanat

Faceți clic pe Caută pentru a selecta anumite directoare şi/sau fişiere de pe calculatorul dumneavoastră.

Următoarele opțiuni sunt disponibile:

Opțiune	*Descriere*
Scanează toate obiectele selectate	Selectați această opțiune pentru a scana doar obiectele selectate anterior.
Programe	Selectați această opțiune pentru a scana doar programe şi aplicații.
Scanează doar extensiile definite de utilizator	Selectați această opțiune pentru a scana doar extensiile de fişiere specificate de dumneavoastră. Va apărea o căsuță de text unde puteți introduce aceste extensii.

Opțiune	Descriere
	Notă Extensiile trebuie separate prin punct şi virgulă (ex: exe;com;ivd;).

Faceți clic pe **Înainte** pentru a continua sau pe **Anulare** dacă doriți să părăsiți programul asistent.

Pasul 3/4 - Selectați acțiunile care vor fi luate

Aici puteți alege ce acțiuni trebuie luate împotriva amenințărilor detectate şi puteți selecta opțiunile de scanare mutând cursorul.

Selectați acțiunile care vor fi luate

Puteți selecta din meniul corespunzător acțiunea care să fie luată:

- **Când este detectat un fişier infectat**

- **Când este detectat un fişier suspect**
- **Când este detectat un fişier ascuns**

De asemenea, puteți configura nivelul de scanare. Puteți alege nivelul de protecție adecvat nevoilor dumneavoastră de securitate. Mutați cursorul pentru a seta nivelul de protecție dorit.

Există patru nivele de protecție:

Nivel de protecție	*Descriere*
Ridicat	Oferă protecție avansată. Consumul de resurse este ridicat. ■ scanează toate fişierele şi arhivele ■ scanează împotriva viruşilor şi a aplicațiilor spyware. ■ scanează după fişiere şi procese ascunse
Mediu	Oferă protecție standard. Consumul de resurse este moderat. ■ scanează toate fişierele ■ scanează împotriva viruşilor şi a aplicațiilor spyware.
Scăzut	Acoperă nevoile elementare de securitate. Consumul de resurse este foarte scăzut. ■ scanează doar aplicații ■ scanează împotriva viruşilor
Personalizat	Permite selectarea propriilor opțiuni de scanare. Faceți clic pe Personalizează şi setați nivelul de scanare. Selectați căsuțele corespunzătoare fiecărui tip de malware care doriți să fie căutat pe calculatorul dumneavoastră în timpul procesului de scanare.

Faceți clic pe **Înainte** pentru a continua sau pe **Anulare** dacă doriți să părăsiți programul asistent.

Pasul 4/4 - Setați opțiuni adiționale

Aici puteți seta opțiuni suplimentare înainte de a iniția scanarea.

Setați opțiuni adiționale

Pentru a salva sarcina de scanare cu scopul de a o folosi ca atare în viitor, selectați căsuța corespunzătoare şi introduceți un nume convenabil în căsuța de text.

Notã
Un buton cu numele specificat de dumneavoastră va apărea în meniul cu sarcini.

Dacă doriți să închideți calculatorul după scanare, selectați căsuța corespunzătoare.

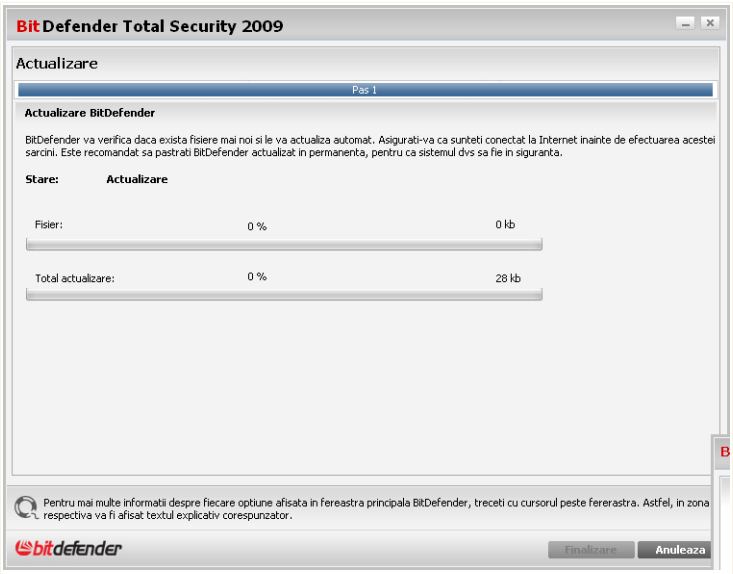
Faceți clic pe **Scanează** şi urmați programul asistent în trei paşi pentru a realiza procesul de scanare.

6.2.2. Actualizarea BitDefender

În fiecare zi sunt descoperite şi 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 şi 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 şi 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 şi, în acelaşi 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.

6.2.3. Verificare vulnerabilități

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

Pentru a verifica dacă sistemul dumneavoastră este vulnerabil, faceți clic pe **Verificare vulnerabilități** şi urmați paşii programului asistent.

Căutare după vulnerabilități

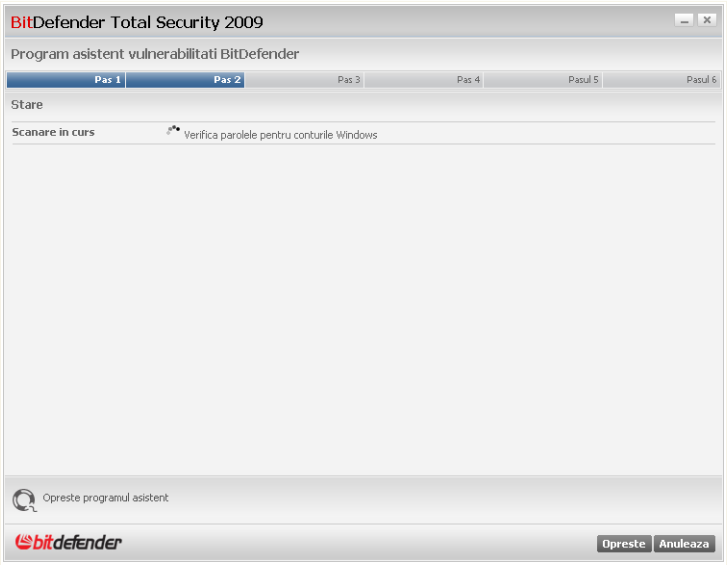
Pentru a verifica dacă sistemul dumneavoastră este vulnerabil, faceți clic pe **Verifică acum** şi urmați paşii programului asistent.

Pasul 1/6 - Selectați vulnerabilitățile de verificat

Vulnerabilități

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

Pasul 2/6 - Căutare vulnerabilități



Căutare vulnerabilități

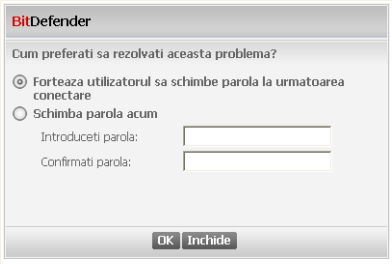
Aşteptați ca BitDefender să finalizeze căutarea.

Pasul 3/6 - Schimbați parolele slabe

Parole utilizatori

Puteti vedea lista conturilor de utilizator Windows configurate pe calculatorul dumneavoastră şi de nivelul de protecție asigurat de parola acestora.

Faceți clic pe **Repară** 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.

Notă
Pentru a crea o parolă puternică, utilizați o combinație de litere mari şi mici, numere şi caractere speciale (cum ar fi #, $ sau @).

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

Faceți clic pe **Înainte**.

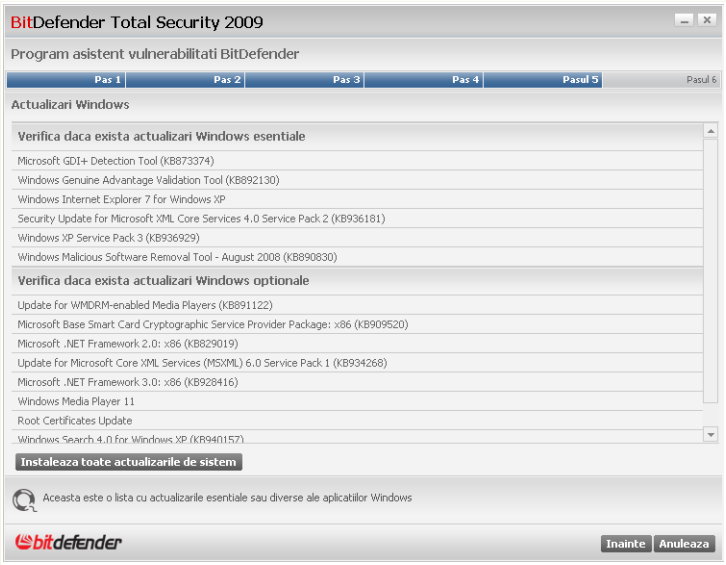
Pasul 4/6 - Actualizaţi aplicaţii

Aplicaţii

Puteţi vedea lista aplicaţiilor verificate de BitDefender şi dacă acestea sunt la zi. Dacă o aplicaţie nu este la zi, faceţi clic pe linkul furnizat pentru a descărca ultima versiune a acesteia.

Faceţi clic pe **Înainte**.

Pasul 5/6 - Actualizaţi Windows



Actualizări Windows

Puteți vedea lista actualizărilor critice şi 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**.

Pasul 6/6 - Examinați rezultatele

Rezultate

Faceți clic pe **Închide**.

7. Optimizare PC

BitDefender conține un modul de Optimizare PC care vă ajută să păstrați integritatea sistemului dumneavoastră. Utilitarele oferite sunt critice pentru îmbunătățirea performanței sistemului dumneavoastră şi gestionarea eficientă a spațiului pe hard disc.

Pentru a executa operații de mentenanță asupra calculatorului dumneavoastră, faceți clic pe tabul **Optimizare PC** şi utilizați funcțiile oferite.

Optimizare

Modulul Optimizare conține două secțiuni:

- **Componente monitorizate** - Vă permite să vedeți lista completă a sarcinilor de optimizare monitorizate. Puteți alege care sarcini să fie monitorizate.
- **Sarcini** - Aici puteți găsi linkuri către cele mai importante sarcini de optimizare: curățare şi recuperare regiştri, ştergerea fişierelor temporare de pe Internet şi a fişierelor cookie, ştergerea fişierelor duplicat, defragmentarea partițiilor locale.

7.1. Componente monitorizate

O singură componentă este monitorizată: Optimizare.

Faceți clic pe căsuța cu semnul "+" pentru a deschide categoria Optimizare sau pe căsuța cu semnul "-" pentru a o închide.

7.1.1. Optimizare

Problemele care ar putea afecta performanța calculatorului dumneavoastră sunt descrise în propoziții explicite. Dacă există astfel de probleme, veți vedea un buton roşu **Repară** în dreptul fiecăreia dintre acestea. Altfel, este afişat un buton verde **OK**.

Problemă	*Descriere*
Nu ați curățat niciodată regiştrii	Asistentul de curățare a regiştrilor scanează regiştrii Windows şi şterge cheile de regiştri nevalide. Curățați regiştrii periodic pentru a creşte performanțele sistemului dumneavoastră.
Nu ați curățat niciodată calculatorul	Curățarea periodică a calculatorului îmbunătățeşte performanțele acestuia. Executați această sarcină cât mai curând posibil.
Nu ați căutat niciodată fişiere duplicate	Asistentul de căutare a fişierelor duplicate optimizează spațiul pe disc descoperind fişierele duplicate de pe sistemul dumneavoastră. Urmați acest asistent cât mai curând posibil.
Nu ați defragmentat niciodată hard discul	Asistentul de defragmentare a discului reorganizează datele de pe hard-disc la nivel fizic astfel încât bucățile care compun fiecare fişier să fie stocate cât mai aproape şi în mod continuu. Defragmentați hard-discul cât mai curând posibil.

Atunci când butoanele de stare au culoarea verde, sistemul dumneavoastră este în siguranță. Pentru a remedia potențialele probleme, urmați aceşti paşi:

1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

Dacă nu doriți ca o anumită problemă să fie monitorizată, debifați căsuța **Da, monitorizează această componentă**.

7.2. Sarcini

Următoarele butoane sunt disponibile:

- **Curăță regiştri** - porneşte programul asistent care vă permite să curățați regiştrii Windows.
- **Recuperează regiştri** - porneşte programul asistent care vă permite să recuperați regiştrii curățați.
- **Distruge fişiere** - porneşte programul asistent care vă permite să ştergeți definitiv fişiere de pe calculatorul dumneavoastră.
- **Curăță fişiere Internet** - porneşte programul asistent care vă permite să ştergeți fişierele Internet temporare şi fişierele cookie.
- **Caută fişiere duplicat** - porneşte programul asistent care vă permite să descoperiți şi să ştergeți fişiere duplicat.
- **Defragmentează partiții** - porneşte programul asistent care vă permite să defragmentați partițiile locale.

7.2.1. Curățarea regiştrilor

Regiştrii Windows sunt o parte importantă a sistemelor de operare Windows. Aceştia reprezintă o bază de date care conține informații şi setări ce privesc componentele hardware şi sistemul de operare, aplicațiile instalate, utilizatorii, preferințele de pe calculatorul dumneavoastă şi altele

Multe aplicații editează chei în regiştrii Windows la instalare. La ştergerea sau dezinstalarea acestor programe, este posibil ca unele dintre cheile de regiştri asociate lor să nu fie şterse, ci să rămână în regiştrii Windows, încetinind sistemul şi chiar cauzând instabilitatea acestuia. La fel se întâmplă atunci când ştergeți scurtături către aplicații instalate sau fişiere ale acestora, precum şi în cazul driverelor corupte.

Pentru a curăța regiştrii Windows şi a îmbunătăți performanțele sistemului dumneavostră, utilizați programul asistent de curățare a regiştrilor. Acesta scanează regiştrii Windows şi şterge cheile de regiştri nevalide.

Pentru a curăța regiştrii Windows, faceți clic pe **Curăță regiştri**. Va trebui să finalizați un program asistent în patru paşi.

Pasul 1/4 - Inițiați scanarea

Aici puteți iniția scanarea regiştrilor.

Stare

Puteți vedea când a fost rulat ultima oară programul asistent şi recomandarea BitDefender.

Faceți clic pe **Înainte**.

Pasul 2/4 - Scanare...

Programul asistent va începe scanarea regiştrilor Windows.

Scanare...

Puteți vedea ultima cheie de regiştri scanată şi statisticile aferente.

Aşteptați ca scanarea cheilor de regiştri să fie finalizată. Dacă doriți să anulați această operație, faceți clic pe **Anulare**.

Notă
Dacă doriți oprirea scanării, faceți clic pe **Opreşte**. Veți sări peste următorul pas.

Pasul 3/4 - Selectați acțiunea

După finalizarea scanării cheilor de regiştri, va apărea o nouă fereastră, unde puteți vedea rezultatele.

Notă
Dacă nu au fost detectate probleme sau dacă ați ales să opriți scanarea, veți sări acest pas.

Acțiuni

Puteți vedea toate cheile de regiştri orfane sau nevalide detectate. Informații detaliate sunt furnizate despre fiecare cheie de regiştri (nume, valoare, prioritate, categorie).

Cheile de regiştri sunt grupate în funcție de locația lor în regiştrii Windows:

Categorie	*Descriere*
Locații aplicații	Chei de regiştri care conțin informații despre calea către aplicațiile instalate pe calculatorul dumneavoastră. Cheile nevalide au atribuite o prioritate scăzută, ceea ce înseamnă că le puteți şterge fără a le mai analiza.
Extensii de fişier	Chei de regiştri care conțin informații despre extensiile de fişier înregistrate pe calculatorul dumneavoastră. Aceste chei de regiştri sunt utilizate în mod obişnuit pentru a menține asocierile de fişiere (pentru a asigura deschiderea programului corect atunci când deschideți un fişier prin intermediul Windows Explorer). De

Categorie	Descriere
	exemplu, o astfel de cheie de regiştri permite Windows să deschidă un fişier `.doc` în Microsoft Word. Cheile nevalide au atribuite o prioritate scăzută, ceea ce înseamnă că le puteți şterge fără a le mai analiza.
DLL-uri partajate	Chei de regiştri care conțin informații despre locația DLL-urilor (librăriilor de legături dinamice) partajate. DLL-urile conțin funcții care sunt utilizate de aplicațiile instalate pentru a executa anumite sarcini. Acestea pot fi partajate între mai multe aplicații pentru a reduce cerințele de memorie şi spațiu pe disc. Aceste chei de regiştri devin nevalide atunci când DLL-ul indicat este mutat în altă locație sau şters complet (acest lucru se întâmplă de obicei atunci când dezinstalați un program). Cheile nevalide au atribuite o prioritate medie, ceea ce înseamnă că ştergerea lor poate avea un impact negativ asupra sistemului.

Pentru a gestiona mai uşor procesul de curățare, puteți selecta o categorie din meniu.

Puteți alege să ştergeți toate cheile nevalide din categoria selectată sau doar unele dintre acestea. Dacă bifați **Şterge toate cheile**, toate cheile detectate vor fi şterse. Dacă doriți să ştergeți doar anumite chei, bifați opțiunea **Şterge** corespunzătoare cheilor respective.

Notă
În mod implicit, toate cheile nevalide detectate vor fi şterse.

Faceți clic pe **Înainte**.

Pasul 4/4 - Examinați rezultatele

Aici puteți vedea rezultatele scanării efectuate de programul asistent.

Rezultate

Dacă nu ați ales să ştergeți toate cheile, va fi afişat un mesaj de avertisment. Vă recomandăm să revedeți problemele respective.

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

7.2.2. Recuperarea regiştrilor curățați

Câteodată, după curățarea regiştrilor, pot apărea probleme în funcționarea sistemului de operare sau a unor aplicații, din cauza unor chei de regiştri lipsă. Acest lucru poate fi cauzat de ştergerea unor chei de regiştri folosite în comun de mai multe programe în timpul ultimei curățiri a regiştrilor sau de alte chei şterse. Pentru a rezolva această problemă trebuie să recuperați regiştrii curățați.

Pentru a recupera regiştrii curățați, faceți clic pe **Recuperează regiştri**. Va trebui să finalizați un program asistent în doi paşi.

Important
Doar utilizatorii cu drepturi administrative pe sistem pot recupera regiştrii curățați.

Pasul 1/2 - Inițiați recuperarea regiştrilor

Aici puteți iniția recuperarea regiştrilor.

Stare

Puteți vedea lista momentelor de timp când au fost curățați regiştrii Windows. Selectați momentul de timp corespunzător configurației regiştrilor Windows la care doriți să reveniți.

Pentru a reveni la configurația regiştrilor Windows de la momentul selectat, faceți clic pe **Înainte**.

Avertisment
Recuperarea regiştrilor curățați poate duce la suprascrierea cheilor de regiştri editate de la ultima curățare.

Pasul 2/2 - Examinați rezultatele

Aici puteți vedea dacă recuperarea a fost efectuată cu succes.

Rezultate

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

7.2.3. Ştergerea permanentă a fişierelor

Atunci când ştergeți un fişier, acesta nu mai poate fi accesat prin mijloace normale. Cu toate acestea, fişierul continuă să existe pe hard disc până ce este suprascris prin copierea altor fişiere.

Chiar dacă ştergeți un fişier, acesta poate fi recuperat utilizând programe specializate. Ca urmare, apare o posibilă ameninţare la adresa datelor dumneavostră personale, deoarece pot exista încercări ale unor persoane răuvoitoare de a recupera aceste date.

Pentru a elimina posibilitatea ca datele cu caracter personal şterse să poată fi recuperate, puteți utiliza BitDefender pentru a şterge la nivel fizic datele respective de pe hard discul dumneavoastră.

Pentru a şterge permanent fişiere, faceți clic pe **Distruge fişiere**. Va trebui să finalizați un program asistent în trei paşi.

Pasul 1/3 - Selectați locația

Aici puteți specifica ce fişiere şi directoare să fie şterse definitiv.

Țintă

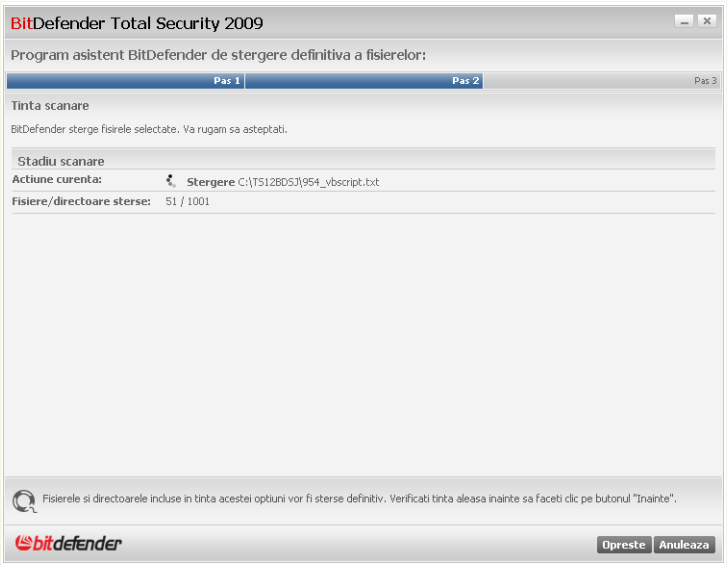
Faceți clic pe **Adaugă locație**, selectați fişierul sau directorul care doriți să fie şters şi faceți clic pe **OK**. Calea către locația selectată va apărea în coloana **Cale**. Dacă vă răzgândiți în legătură cu locația, faceți clic pe butonul **Şterge** de lângă aceasta.

Notă
Puteți selecta una sau mai multe locații.

Faceți clic pe **Înainte**.

Pasul 2/3 - Ştergere fişiere...

BitDefender va şterge definitiv fişierele din locațiile specificate.



Ştergere...

Aşteptaţi finalizarea operaţiei de ştergere ireversibilă a fişierelor. Dacă doriţi să anulaţi această operaţie, faceţi clic pe **Anulare**.

Pasul 3/3 - Examinaţi rezultatele

După ce toate fişierele au fost şterse, va apărea o nouă fereastră, unde puteţi vedea rezultatele.

Rezultate

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

7.2.4. Curățarea fișierelor Internet

De fiecare dată când vizitați o pagină web, sunt create fişiere Internet temporare pentru a permite accesul mai rapid la pagina respectivă data viitoare când o vizitați.

Cu toate că sunt denumite temporare, aceste fişiere nu sunt şterse după ce închideți browserul. Aceasta poate reprezenta o amenințare la adresa intimității dumneavostră, deoarece aceste fişiere pot fi examinate de oricine are acces la calculatorul dumneavoastră. În plus, cu trecerea timpului, aceste fişiere vor ocupa din ce în ce mai mult spațiu pe hard disc.

De asemenea, atunci când vizitați o pagină web, pe calculatorul dumneavostră sunt stocate fişiere cookie. Fişierele cookie sunt fişiere de mici dimensiuni ce conțin informații referitoare la preferințele dumneavostră legate de navigarea pe Internet. Acestea pot fi o amenințare la adresa intimității dumneavoastră, deoarece pot fi

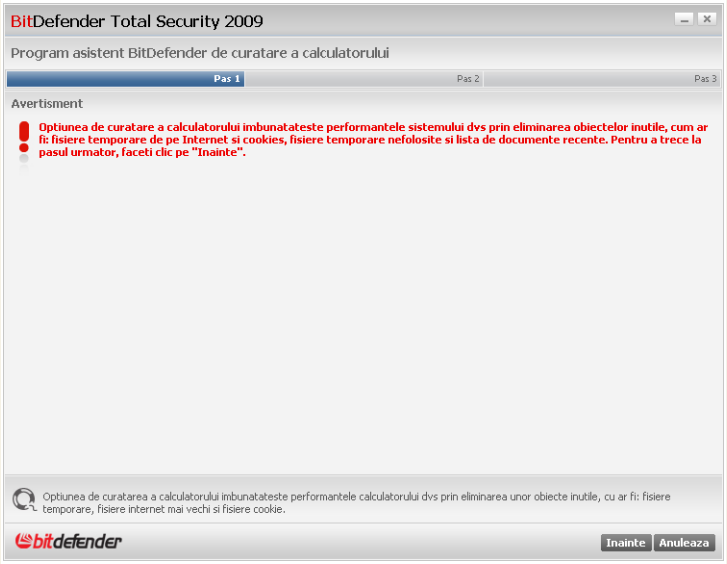
analizate şi folosite de specialişti în publicitate pentru a vă urmări interesele şi gusturile privitoare la Internet.

Prin ştergerea fişierelor Internet temporare şi a fişierelor cookie, veți avea mai mult spațiu liber pe disc şi vă veți proteja intimitatea.

Pentru a şterge directorul Temporary Internet Files, unde Internet Explorer păstrează fişierele Internet temporare şi fişierele cookie, faceți clic pe **Şterge fişiere Internet**. Va trebui să finalizați un program asistent în trei paşi.

Pasul 1/3 - Inițiați ştergerea

Aici puteți iniția ştergerea fişierelor Internet temporare şi a fişierelor cookie.



Fereastra de întâmpinare

Faceți clic pe **Înainte**.

Pasul 2/3 - Ştergere fişiere...

Programul asistent va începe ştergerea fişierelor Internet temporare şi a fişierelor cookie.

Ştergere fişiere...

Aşteptaţi ca fişierele Internet temporare şi fişierele cookie să fie şterse. Dacă doriţi să anulaţi această operaţie, faceţi clic pe **Anulare**.

Pasul 3/3 - Examinaţi rezultatele

După ce toate fişierele au fost şterse, va apărea o nouă fereastră, unde puteţi vedea rezultatele.

Rezultate

Puteți vedea statisticile referitoare la fişierele şterse.

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

7.2.5. Depistarea fişierelor duplicat

Fişierele duplică consumă spațiul hard discului dumneavoastră. Gândiți-vă doar că ați avea acelaşi fişier `.mp3` stocat în trei locații diferite.

Pentru a detecta şi şterge fişierele duplicat de pe calculatorul dumneavoastră, puteți utiliza programul asistent de depistare a duplicatelor. În acest fel puteți gestiona mai bine spațiul liber de pe hard discul dumneavoastră.

Pentru a căuta fişiere duplicat, faceți clic pe **Caută fişiere duplicat**. Va trebui să finalizați un program asistent în patru paşi.

Pasul 1/4 - Selectați locația căutării

Aici puteți specifica unde să fie căutate fişiere duplicat.

Locație căutare

Faceți clic pe **Caută** şi selectați o locație unde programul asistent să caute fişiere duplicat. Calea către locația selectată va apărea în coloana **Cale**. Dacă vă răzgândiți în legătură cu locația, faceți clic pe butonul **Şterge** de lângă aceasta.

Notă
Puteți selecta una sau mai multe locații.

Faceți clic pe **Înainte**.

Pasul 2/4 - Căutare...

Programul asistent va începe să caute fişiere duplicat.

Căutare...

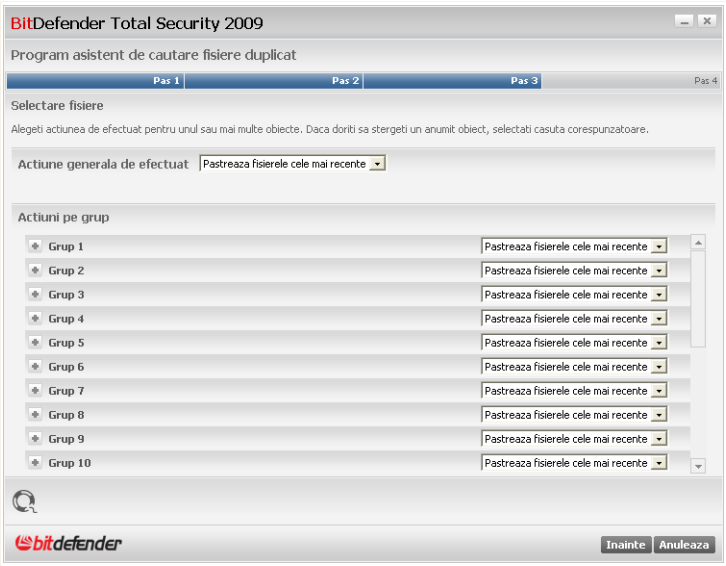
Puteți vedea stadiul şi statisticile căutării.

Aşteptați să fie finalizată căutarea de fişiere duplicat. Dacă doriți să anulați această operație, faceți clic pe **Anulare**.

Pasul 3/4 - Selectați acțiunea

După ce căutarea a fost finalizată, va apărea o nouă fereastră, unde puteți specifica ce acțiuni să fie luate asupra fişierelor duplicat detectate.

Notă
Dacă nu au fost detectate fişiere duplicat, veți sări acest pas.



Acțiuni

Fişierele duplicat detectate sunt organizate şi afişate în grupuri. Dacă faceți clic pe căsuța corespunzătoare unui grup, puteți vedea informații detaliate despre fişierele duplicat (calea completă, dimensiunea, data creării şi modificării).

Puteți alege o acțiune globală care să fie aplicată tuturor fişierelor duplicat detectate sau puteți alege acțiuni care să fie aplicate pe grupuri de fişiere duplicat. Următoarele acțiuni sunt disponibile pe meniu:

Acțiune	*Descriere*
Păstrează cel mai recent fişier	Va fi păstrat cel mai recent duplicat, în timp ce celelalte vor fi şterse.
Păstrează cel mai vechi fişier	Va fi păstrat cel mai vechi duplicat, în timp ce celelalte vor fi şterse.
Nicio acțiune	Nu se va aplica nicio acțiune fişierelor detectate.

Dacă doriți să aplicați o acțiune globală tuturor obiectelor dintr-un grup, selectați acțiunea dorită din meniul corespunzător. Dacă doriți ca doar anumite fişiere dintr-un grup să fie şterse, bifați opțiunea **Şterge** corespunzătoare fişierelor respective.

Notă

Acțiunea globală nu va suprascrie acțiunea aleasă pentru anumite grupuri sau fişiere. Aceasta înseamnă, de exemplu, că dacă setați ca acțiune globală **Păstrează cel mai recent fişier**, dar specificați să nu fie aplicată nicio acțiune unui anumit grup, atunci acțiunea globală va fi aplicată tuturor grupurilor cu excepția acestuia.

Faceți clic pe **Înainte**.

Pasul 4/4 - Examinați rezultatele

Aici puteți vedea rezultatele scanării după fişiere duplicat.

Rezultate

Faceți clic pe **Execută din nou** pentru a porni o nouă căutare de fişiere duplicat sau pe **OK** pentru a închide fereastra.

7.2.6. Defragmentarea volumelor hard-discului

La copierea unui fişier ce depăşeşte mărimea celui mai mare bloc de spațiu liber pe hard-disc se produce fragmentarea fişierului. Deoarece nu este îndeajuns spațiu liber continuu pentru a stoca întregul fişier, acesta va fi stocat în mai multe blocuri. Atunci când fişierul fragmentat este accesat, informația conținută de acesta este citită din mai multe locații diferite.

Fragmentarea fişierelor încetineşte accesul la fişiere şi scade performanța sistemului. De asemenea, aceasta accelerează uzura hard-discului.

Pentru a diminua gradul de fragmentare al fişierelor trebuie să defragmentați hard-discul periodic. Prin defragmentare, informațiile de pe hard-disc sunt reorganizate la nivel fizic astfel încât bucățile ce compun fiecare fişier să fie stocate cât mai aproape şi în mod continuu. De asemenea, prin defragmentare, se încearcă crearea unor porțiuni cât mai mari de spațiu liber, pentru a preveni fragmentarea ulterioară a fişierelor.

Defragmentarea hard-discului este recomandată pentru:

- accesarea mai rapidă a fişierelor.
- îmbunătățirea performanței globale a sistemului.
- extinderea duratei de viață a hard-discului.

Pentru a defragmenta hard discul, faceți clic pe **Defragmentează partiții**. Va trebui să finalizați un program asistent în trei paşi.

Notă
Defragmentarea poate dura destul de mult deoarece implică mutarea unor blocuri de date dintr-un loc în altul pe hard disc. Este recomandat să inițiați defragmentarea atunci când nu utilizați calculatorul.

Step 1/3 - Analizare...

Programul asistent de defragmentare va analiza hard discul pentru a stabili dacă trebuie defragmentat sau nu.

Analizare

Aşteptați ca analiza să fie finalizată. Dacă doriți să anulați această operație, faceți clic pe **Anulare**.

Pasul 2/3 - Examinați raportul de analiză

După finalizarea analizei, va apărea o nouă fereastră, unde puteți vedea rezultatele analizei şi puteți iniția defragmentarea hard discului, dacă aceasta este necesară.

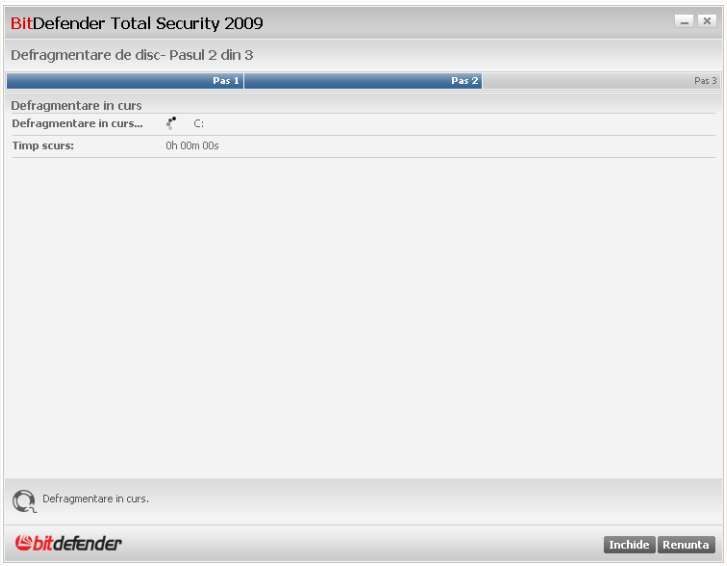
Raportul de analiză

Verificați raportul de analiză.

Dacă nicio partiție nu necesită defragmentare, faceți clic pe **Închide** pentru a închide fereastra. Altfel, selectați opțiunea **Defragmentează** corespunzătoare partițiilor care necesită defragmentare şi faceți clic pe **Execută** pentru a inița defragmentarea.

Notă

Pentru a putea defragmenta un volum este necesar ca un procent de 15% din acesta să fie spațiu liber. Dacă nu este îndeajuns spațiu liber pe volumul ce trebuie defragmentat, atunci defragmentarea va fi abandonată.



Defragmentare

Aşteptați ca defragmentarea hard discului să fie finalizată. Puteți anula defragmentarea în orice moment făcând clic pe **Închide**.

Pasul 3/3 - Examinați raportul defragmentării

După ce defragmentarea hard discului a fost finalizată, va apărea o nouă fereastră, unde puteți vedea statisticile defragmentării.

Raportul defragmentării

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

8. Administrare fişiere

BitDefender include un modul Administrare fişiere care vă ajută să păstraţi confidenţialitatea datelor dumneavoastră. În acest scop, faceţi copii de siguranţă la fişierele dumneavoastră şi utilizaţi seifurile de fişiere.

Backup. Protecţia antivirus singură nu mai este suficientă pentru protejarea datelor dumneavoastră confidenţiale. Imaginaţi-vă că sistemul dumneavoastră nu este virusat, dar calculatorul se defectează prematur atunci când aveţi nevoie cel mai mult de acesta. Aici vă este utilă secţiunea Backup a modulului Administrare fişiere. Puteţi face copii de siguranţă a fişierelor dumneavoastră cu ajutorul BitDefender.

Seif de fişiere. Secţiunea Seif de fişiere a modulului Administrare fişiere vă ajută să vă protejaţi fişierele confidenţiale.

- Seiful de fişiere reprezintă un spaţiu sigur de stocare a informaţiilor personale sau a fişierelor confidenţiale.
- Seiful de fişiere este de fapt un fişier criptat de pe calculatorul dumneavoastră, având extensia bvd.
- Seiful de fişiere fiind criptat, datele dinăuntrul acestuia sunt protejate împotriva furtului sau a altor pericole informatice.
- Atunci când deschideţi acest fişier bvd, va apărea o nouă partiţie logică (un nou drive). Veţi înţelege mai uşor procesul prin analogie cu un proces similar: montarea unei imagini ISO ca CD virtual.

Deschideţi My Computer şi veţi vedea un nou drive, care corespunde seifului dumneavoastră de fişiere. Puteţi face diverse operaţii cu fişierele din seif (copiere, ştergere, modificare etc). Fişierele sunt protejate cât timp se află în acest drive (deoarece este nevoie de parolă pentru deschiderea acestuia). Atunci când aţi terminat ce aveaţi de făcut, închideţi seiful pentru a proteja conţinutul acestuia.

Pentru a accesa modulul Administrare fişiere, faceţi clic pe tabul **Administrare fişiere**.

Administrare fişiere

Modulul Administrare fişiere conține două secțiuni:

- **Componente monitorizate** - Vă permite să vedeți lista completă a componentelor monitorizate pentru fiecare modul. Puteți alege care dintre module să fie monitorizate. Este recomandată monitorizarea tuturor componentelor.
- **Sarcini** - Aici puteți găsi linkuri către cele mai importante sarcini de securitate: backup şi restaurare locală, adăugare, vizualizare şi ştergere seifuri de fişiere.

8.1. Componente monitorizate

Componentele monitorizate sunt grupate în mai multe categorii.

Componenta monitorizată este următoarea:

Categorie	Descriere
Seif de fişiere	Este un spațiu sigur de stocare a informațiilor personale sau a fişierelor confidențiale de pe calculatorul dumneavoastră.

Categorie	Descriere
	Deoarece seiful este criptat, datele dinăuntrul acestuia sunt protejate împotriva furtului şi a altor pericole informatice.
Backup	Vă ajută să faceți copii de rezervă pentru orice date importante de pe sistemul dumneavoastră. Este recomandat să utilizați această capabilitate pentru a vă păstra în siguranță datele importante.

Faceți clic pe semnul “+” pentru a deschide o categorie sau pe “-” pentru a închide categoria.

8.1.1. Seif de fișiere

Problemele privind confidențialitatea datelor dumneavoastră sunt descrise în propoziții explicite. Dacă există astfel de probleme, veți vedea un buton roşu **Repară** în dreptul fiecăreia dintre acestea. Altfel, este afişat un buton verde **OK**.

Problemă	Descriere
Seiful de fişiere este activat	Seiful de fişiere păstrează confidențialitatea documentelor dumneavoastră criptându-le în seife speciale de fişiere.

Atunci când butoanele de stare au culoarea verde, datele dumneavoastră sunt în siguranță. Pentru a remedia potențialele probleme, urmați aceşti paşi:

1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

Dacă nu doriți ca o anumită problemă să fie monitorizată, debifați căsuța **Da, monitorizează această componentă**.

8.1.2. Backup

Problemele care ar putea afecta siguranța datelor dumneavoastră sunt descrise în propoziții explicite. Dacă există astfel de probleme, veți vedea un buton roşu **Repară** în dreptul fiecăreia dintre acestea. Altfel, este afişat un buton verde **OK**.

Problemă	Descriere
Ați executat o sarcină de backup local pe calculatorul dumneavoastră cu x zile în urmă	Modulul de backup local vă ajută să faceți copii de rezervă pentru orice date importante de pe sistemul dumneavoastră.

Atunci când butoanele de stare au culoarea verde, datele dumneavoastră sunt în siguranță. Pentru a remedia potențialele probleme, urmați aceşti paşi:

1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

Dacă nu doriți ca o anumită problemă să fie monitorizată, debifați căsuța **Da, monitorizează această componentă**.

8.2. Sarcini

Următoarele butoane sunt disponibile:

- **Backup local** - porneşte programul asistent care vă permite să faceți copii de rezervă pentru orice date importante pe calculatorul dumneavoastră, pe un CD, la o locație din rețea sau pe alt hard disc.
- **Restaurare locală** - porneşte programul asistent care vă permite să restaurați datele pentru care au fost făcute anterior copii de siguranță pe calculatorul dumneavoastră, pe un CD, la o locație din rețea sau pe alt hard disc.
- **Setări backup** - aici puteți seta şi executa operațiuni de backup în detaliu.

Notă
Pentru mai multe informații, consultați "*Opțiuni avansate de backup*" (p. 301).

- **Adaugă fişier în seif** - porneşte programul asistent care vă permite să stocați în siguranță fişierele / documentele dumneavoastră importante criptându-le în partiții special, securizate (seife de fişiere).
- **Şterge fişiere din seif** - porneşte programul asistent care vă permite să ştergeți date din seiful de fişiere.

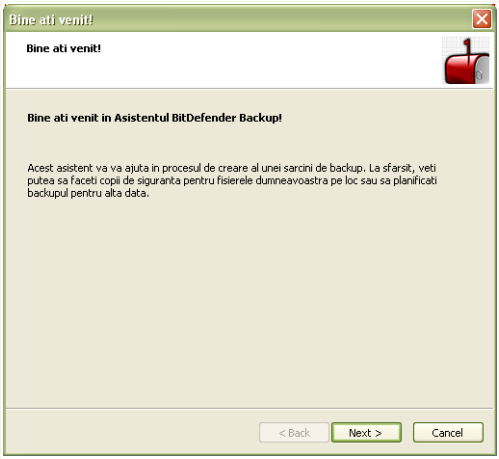
- **Afişează seif** - porneşte programul asistent care vă permite să vedeți conținutul seifurilor dumneavoastră de fişiere.
- **Închide seif** - porneşte programul asistent care vă permite să vă închideți seiful pentru a proteja conținutul acestuia.

8.2.1. Crearea de copii de siguranță local

Făcând clic pe **Backup local**, veți fi ghidat de către un program asistent prin procesul de creare a unei sarcini de backup local. La sfârşitul acestui proces, veți putea face copii de siguranță pentru fişiere pe loc sau puteți programa produsul să le facă mai târziu.

Pasul 1/5 - Fereastra de întâmpinare

Aceasta este doar o pagină de bun venit.

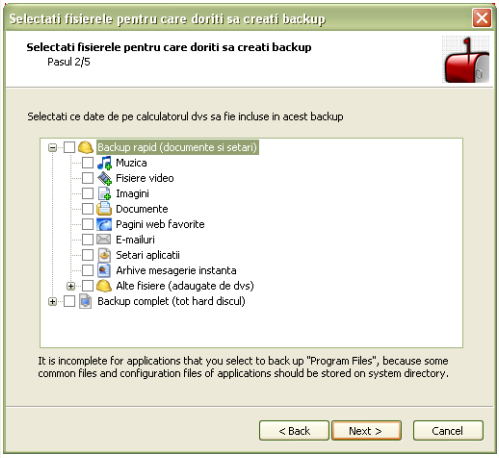


Fereastra de întâmpinare

Faceți clic pe **Înainte**.

Pasul 2/5 - Alegeți la ce să faceți backup

Aici puteți selecta datele de pe calculatorul dumneavoastră la care să faceți copii de rezervă.



Alegeți la ce anume să faceți backup

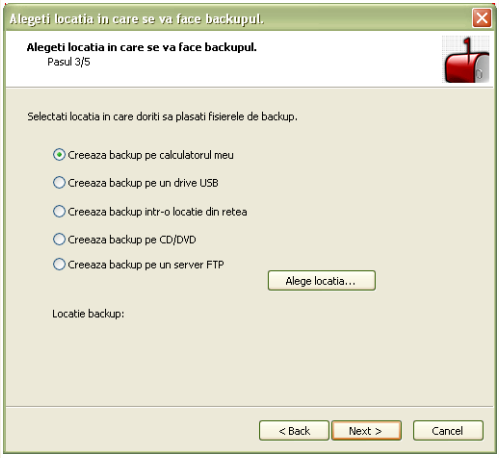
Puteți alege fie **Backup rapid** (muzica, fişierele video, pozele, mesajele email, setările aplicațiilor etc.), fie **Backup complet** (toate partițiile).

Faceți clic pe **Alte fişiere** pentru a adăuga alte fişiere de pe desktopul dumneavoastră la **Backup rapid**. De asemenea, **Backupul complet** poate fi uşor personalizat, selectând directoarele dintr-o anumită partiție pentru care să se facă backup.

Faceți clic pe **Înainte**.

Pasul 3/5 - Alegeți unde să faceți backup

Aici puteți selecta locația copiilor de rezervă.



Alegeți unde să faceți backup

Următoarele opțiuni sunt disponibile:

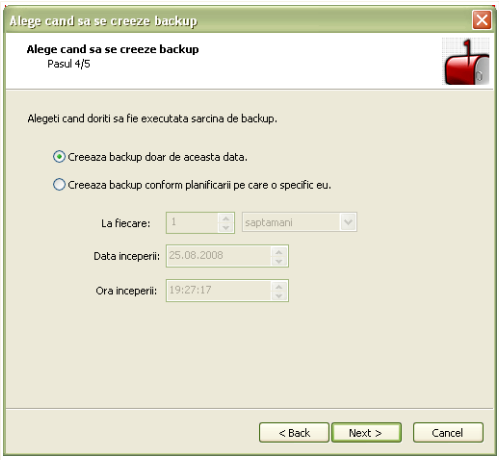
- **Creează backup pe calculator**
- **Creează backup pe un drive USB**
- **Creează backup într-o locație din rețea**
- **Creează backup pe CD/DVD**
- **Creează backup pe un server de FTP**

Dacă decideți să faceți backup pe calculatorul dumneavoastră, pe USB sau pe o locație din rețea, faceți clic pe **Alegeți locație** şi selectați unde să salvați datele.

Faceți clic pe **Înainte**.

Pasul 4/5 - Alegeți când să fie făcut backupul

Aici puteți alege când să fie efectuat backupul.



Alegeți când să fie făcut backupul

Următoarele opțiuni sunt disponibile:

- **Creează backup doar de această dată**
- **Creează backup pe baza programului specificat**

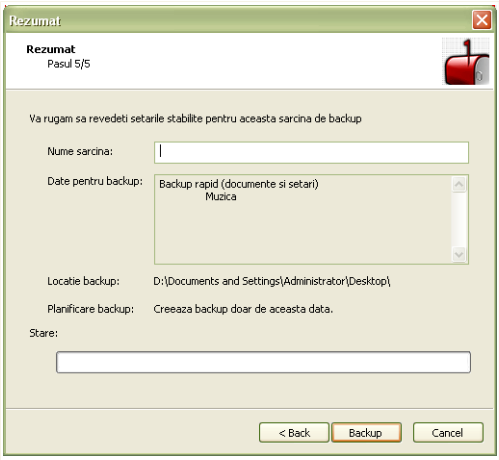
Pentru a face backup la datele dumneavoastră imediat, faceți clic pe **Creează backup doar de această dată**, pentru a programa produsul să facă backup la fişierele dumneavoastră la un moment ulterior, faceți clic pe **Creează backup pe baza programului specificat**.

Dacă selectați **Creează backup pe baza programului specificat**, puteți specifica frecvența cu care să ruleze sarcina programată: zilnic sau săptămânal. De asemenea, puteți specifica momentul şi data la care aceasta să înceapă.

Faceți clic pe **Înainte**.

Pasul 5/5 - Rezumat

Aici puteți revedea setările sarcinii de backup.



Rezumat

Trebuie să introduceți numele sarcinii în câmpul corespunzător.

Faceți clic pe **Backup** dacă sunteți mulțumit de setări.

Faceți clic pe **Finalizare**.

8.2.2. Restaurarea copiilor de siguranță locale

Făcând clic pe **Backup local**, veți fi ghidat de către un program asistent prin procesul de restaurare a copiilor de siguranță locale.

Pasul 1/4 - Fereastra de întâmpinare

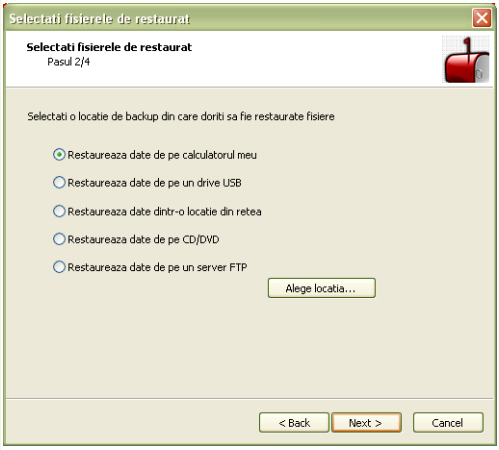
Aceasta este doar o pagină de bun venit.

Fereastra de întâmpinare

Faceți clic pe **Înainte**.

Pasul 2/4 - Alegeți la ce să fie făcut backup

Aici puteți selecta o locație de unde să restaurați fişiere.



Alegeți la ce să fie făcut backup

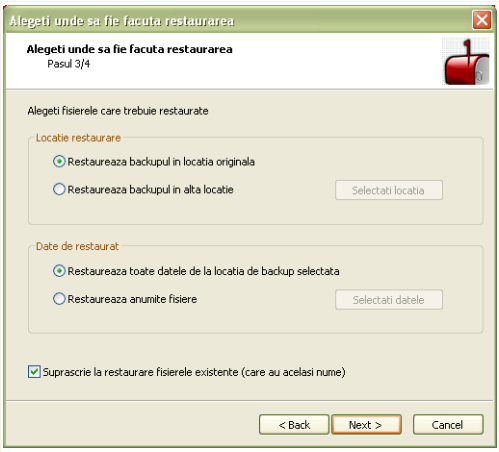
Următoarele opțiuni sunt disponibile:

- **Restaurează date de pe calculator**
- **Restaurează date de pe un drive USB**
- **Restaurează date dintr-o locație din rețea**
- **Restaurează date de pe CD/DVD**
- **Restaurează date de pe un server de FTP**

Faceți clic pe **Înainte**.

Pasul 3/4 - Alegeți locația și fișierele pentru restaurare

Aici puteți alege care fişiere să fie restaurate şi unde doriți să fie restaurate.



Alegeți locația de restaurare și fișierele restaurate

Următoarele opțiuni sunt disponibile:

- **Restaurează backup în locația originală**
- **Restaurează backupul în altă locație**
- **Restaurează toate datele din locația de backup selectată**
- **Restaurează anumite fișiere**
- **Suprascrie la restaurare fișierele existente**

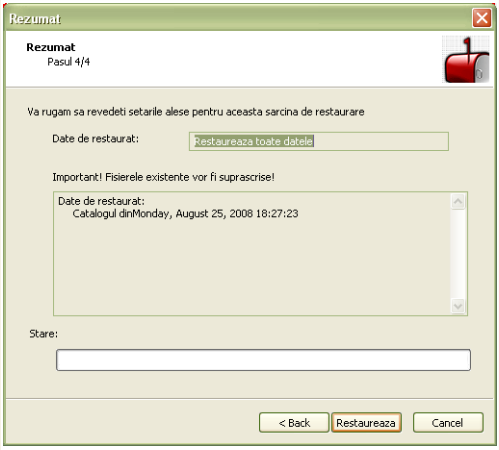
Dacă doriți să restaurați date în altă locație sau doar anumite fișiere, selectați locația și datele făcând clic pe butonul corespunzător.

Pentru a evita suprascrierea fișierului existent la restaurare, debifați căsuța **Suprascrie la restaurare fișierele existente**.

Faceți clic pe **Înainte**.

Pasul 4/4 - Rezumat

Aici puteți revedea setările sarcinii de restaurare.



Faceți clic pe **Restaurează** dacă sunteți mulțumit de setări.

Faceți clic pe **Finalizare**.

8.2.3. Adăugarea fișierelor în seif

Seiful de fişiere este o locație specială utilizată pentru stocarea în siguranță a datelor importante. Documentele dintr-un seif de fişier sunt criptate.

Făcând clic pe **Adaugă fişiere în seif**, veți fi ghidat de către un program asistent prin procesul de creare a unui seif şi de adăugare de documente în acesta.

Pasul 1/6 - Selectați locația

Aici puteți specifica fişierele şi directoarele care să fie adăugate în seif.

Țintă

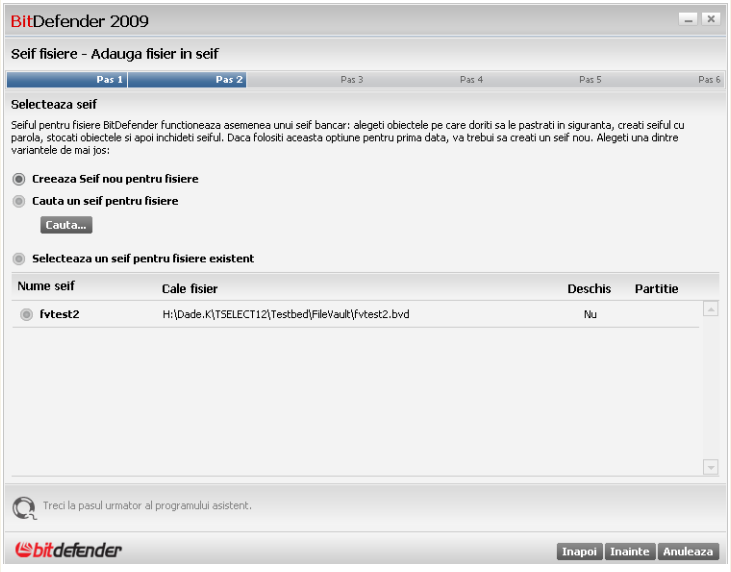
Faceți clic pe **Adaugă locație**, selectați fișierul sau directorul care doriți să fie adăugat şi faceți clic pe **OK**. Calea către locația selectată va apărea în coloana **Cale**. Dacă vă răzgândiți în legătură cu locația, faceți clic pe butonul **Şterge** de lângă aceasta.

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 fişiere**, trebuie să faceți clic pe **Caută** şi să selectați seiful de fişiere. Veți merge la pasul 5 dacă seiful selectat este deschis sau la pasul 4 dacă este închis.

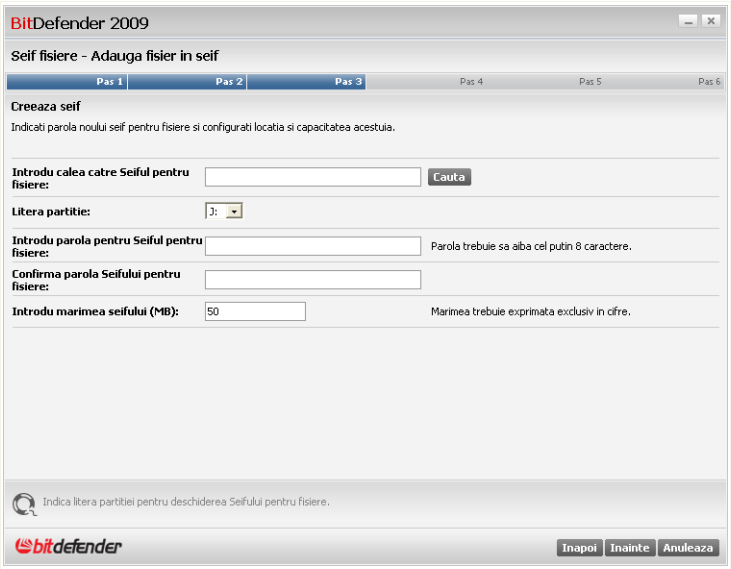
Dacă faceți clic pe **Selectează un seif de fişiere existent**, trebuie să faceți clic apoi pe numele seifului dorit. Veți merge la pasul 5 dacă seiful selectat este deschis sau la pasul 4 dacă este închis.

Selectați **Creează un nou seif de fişiere** 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 fişiere, urmați aceşti paşi:

1. Faceți clic pe **Caută** şi alegeți o locație pentru fişierul bvd.

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

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

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

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

Notă
Parola trebuie să conțină minim 8 caractere.

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

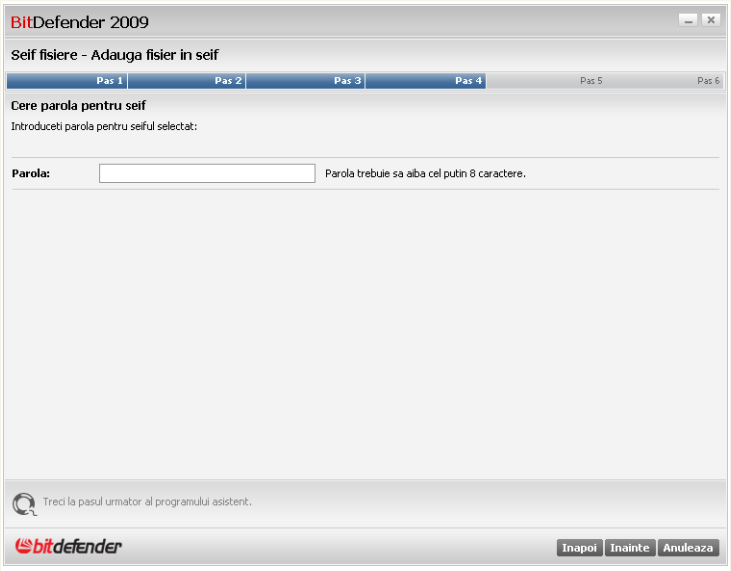
Notă
Dimensiunea trebuie să conțină doar cifre.

Faceți clic pe **Înainte**.

Veți merge la pasul 5.

Pasul 4/6 - Parola

Aici vi se va cere să introduceți parola seifului selectat.

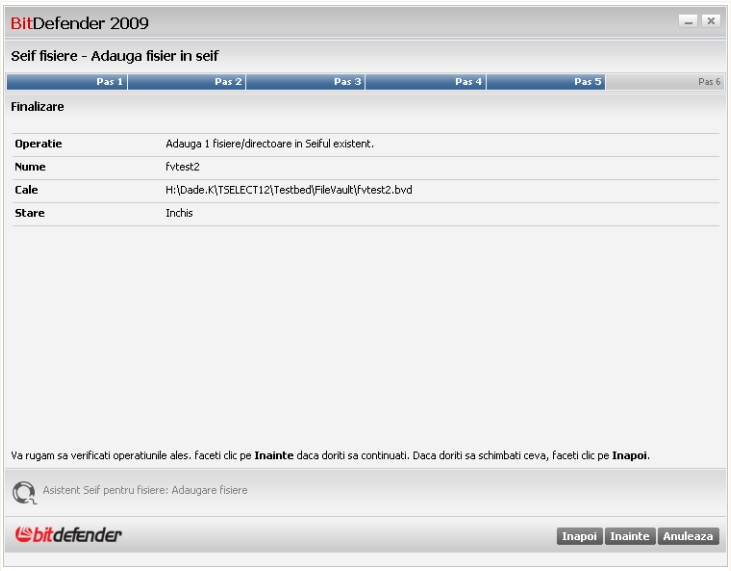


Confirmarea parolei

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

Step 5/6 - Sumar

Aici puteți vedea operațiile alese.

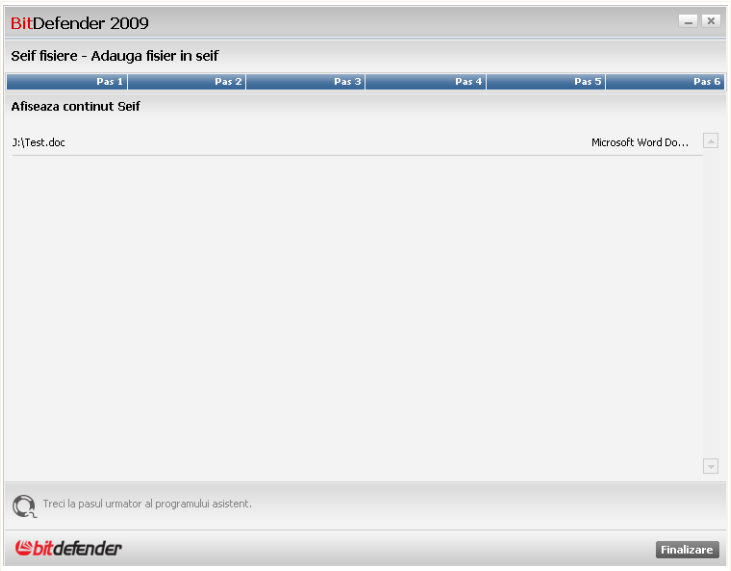


Rezumat

Faceți clic pe **Înainte**.

Pasul 6/6 - Rezultate

Aici puteți vedea conținutul seifului.



Rezultate

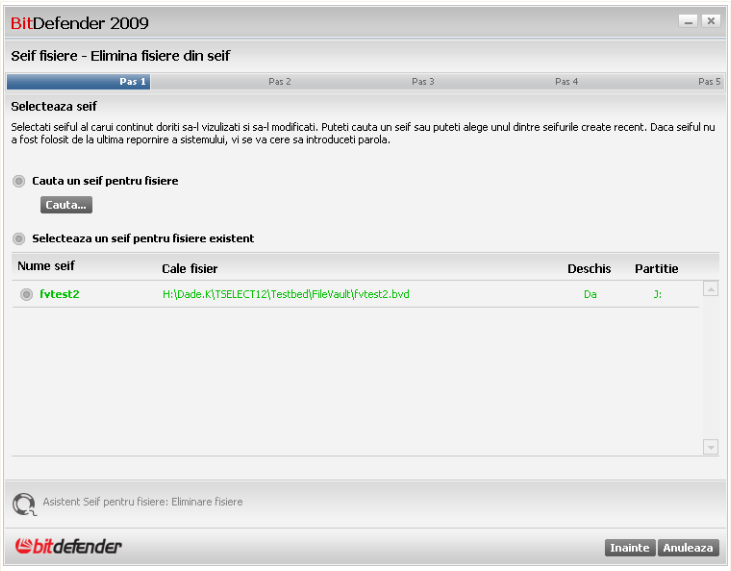
Faceți clic pe **Finalizare**.

8.2.4. Ştergerea fişierelor din seif

Făcând clic pe **Şterge fişiere din seif**, veți fi ghidat de către un program asistent prin procesul de ştergere a fişierelor dintr-un anumit seif.

Pasul 1/5 - Selectați seiful

Aici puteți specifica seiful din care să ştergeți fişiere.



Selectați seiful

Dacă selectați **Caută un seif de fişiere**, trebuie să faceți clic pe **Caută** şi să selectați seiful de fişiere. 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 fişiere 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

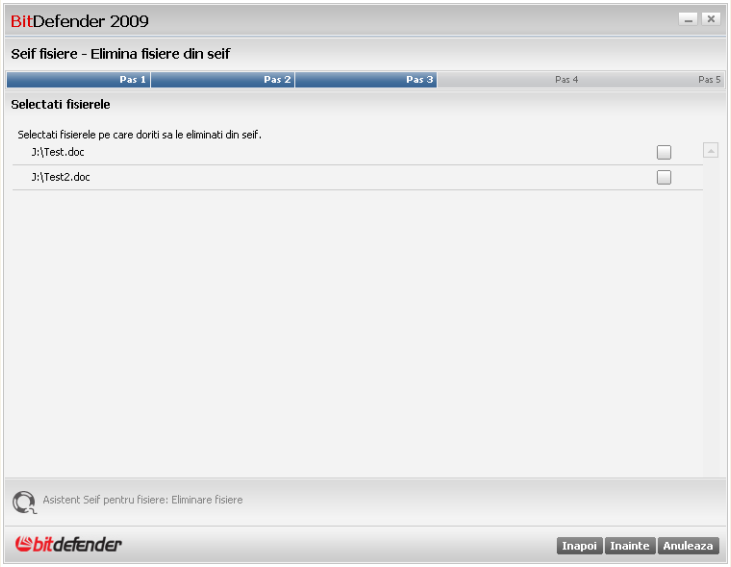
Aici vi se va cere să introduceți parola seifului selectat.

Confirmarea parolei

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

Pasul 3/5 - Selectați fișierele

Aici vor fi afişate fişierele 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

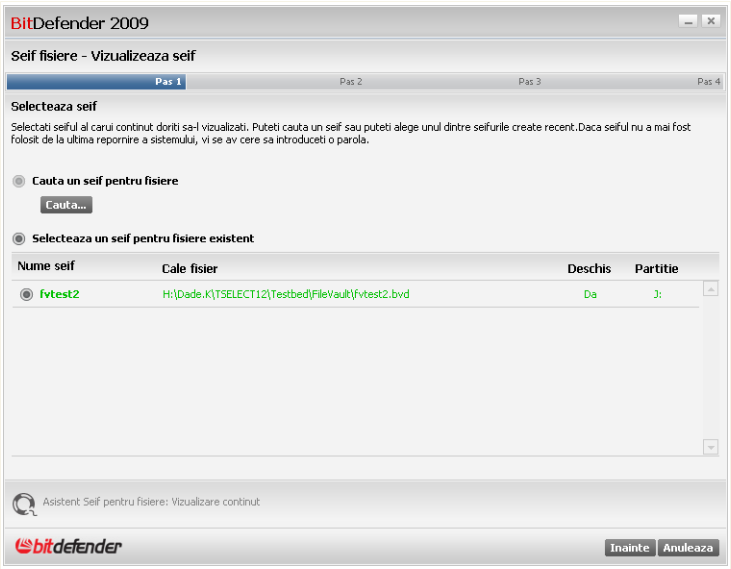
Faceți clic pe **Finalizare**.

8.2.5. Vizualizarea fișierelor din seif

Făcând clic pe **Afişează seif**, veți fi ghidat de către un program asistent prin procesul de vizualizare a fişierelor dintr-un anumit seif.

Pasul 1/4 - Selectați seiful

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



Selectați seiful

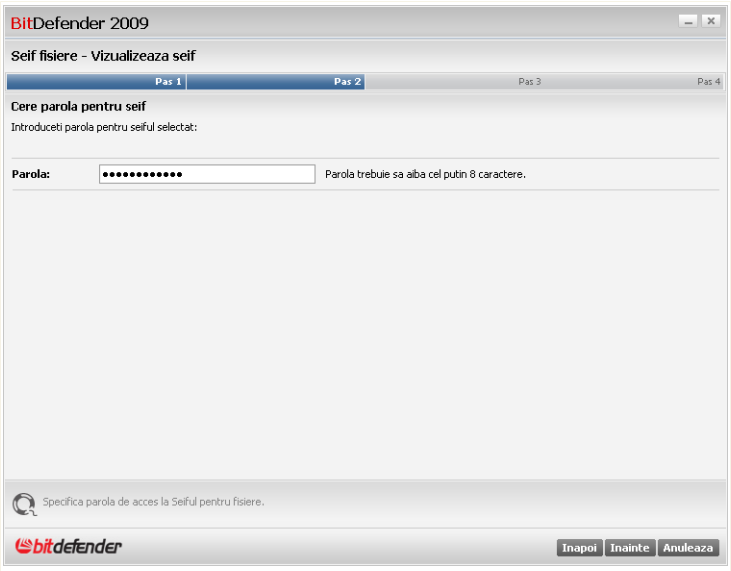
Dacă selectați **Caută un seif de fişiere**, trebuie să faceți clic pe **Caută** şi să selectați seiful de fişiere. Veți merge la pasul 3 dacă seiful selectat este deschis sau la pasul 2 dacă este închis.

Dacă faceți clic pe **Selectează un seif de fişiere 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 şi faceți clic pe **Înainte**.

Pasul 3/4 - Rezumat

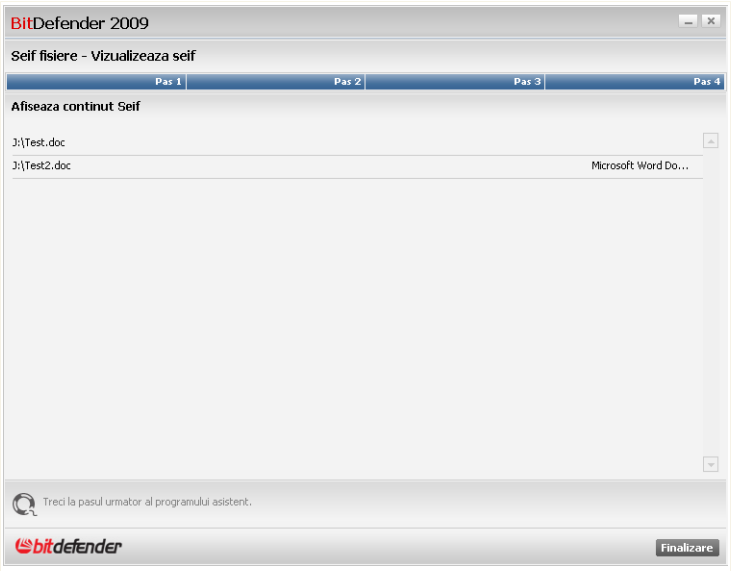
Aici puteți vedea operațiile alese.

Rezumat

Faceți clic pe **Înainte**.

Pasul 4/4 - Rezultate

Aici puteți vedea fişierele din seif.



Rezultate

Faceți clic pe **Finalizare**.

8.2.6. Închiderea seifului

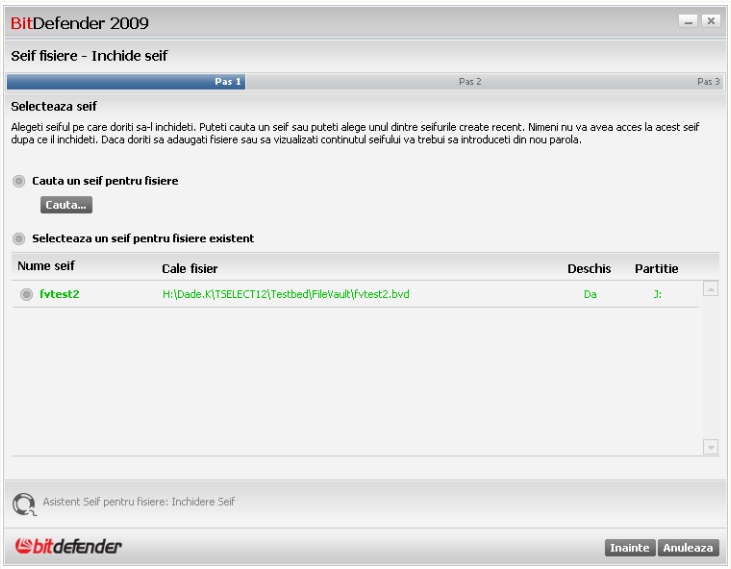
Un seif de fişiere este de fapt un fişier criptat de pe calculatorul dumneavoastră, având extensia bvd. Seiful de fişiere poate fi deschis sau închis.

Pentru a înțelege mai bine acest proces, gândiți-vă la seiful unei bănci - uşa fortificată a acestuia poate fi deschisă sau închisă. Conținutul seifului este protejat doar atunci când uşa este închisă. Analog, conținutul acestuia poate fi accesat doar când este deschis.

Făcând clic pe **Închide seif**, veți fi ghidat de către un program asistent prin procesul de închidere a seifului.

Pasul 1/3 - Selectați seiful

Aici puteți specifica seiful care să fie închis.



Selectați seiful

Dacă selectați **Caută un seif de fişiere**, trebuie să faceți clic pe **Caută** şi să selectați seiful de fişiere.

Dacă faceți clic pe **Selectează un seif de fişiere 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.

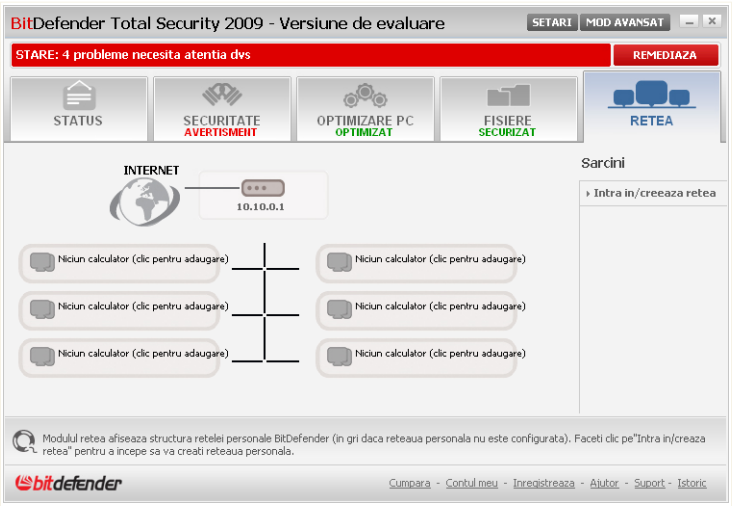
Rezultate

Faceți clic pe **Finalizare**.

9. 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 aceşti paşi:

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 şi intrați în rețea (setați parola).
3. Întoarceți-vă la calculatorul dumneavoastră şi adăugați calculatoarele pe care doriți să le administrați.

9.1. Sarcini

Inițial, un singur buton este disponibil.

- **Intră/Creează rețea** - vă permite să setați parola rețelei, intrând astfel în rețea.

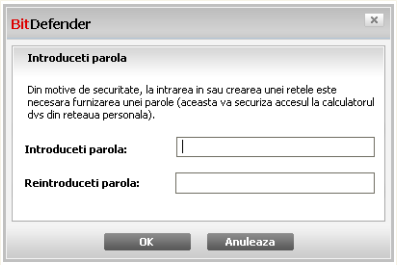
După intrarea în rețea, vor apărea mai multe butoane.

- **Părăseşte rețeaua** - vă permite să părăsiți rețeaua.
- **Administrează rețeaua** - vă permite să adăugați un calculator în rețeaua dumneavoastră.
- **Scanează tot** - vă permite să scanați toate calculatoarele administrate în acelaşi timp.
- **Actualizează tot** - vă permite să actualizați toate calculatoarele administrate în acelaşi timp.
- **Înregistrează tot** - vă permite să înregistrați toate calculatoarele administrate în acelaşi timp.

9.1.1. Intrarea în rețeaua BitDefender

Pentru a în rețeaua BitDefender personală, urmați aceşti paşi:

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



Configurare parolă

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

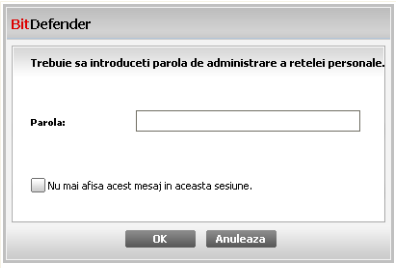
Puteți vedea numele calculatorului apărând pe harta rețelei.

9.1.2. 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.

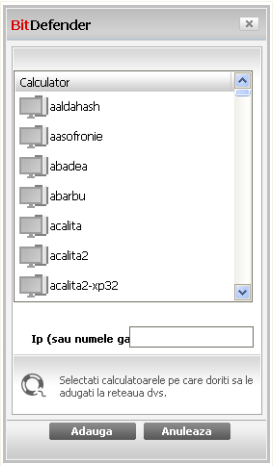
Pentru a adăuga un calculator la rețeaua BitDefender personală, urmați aceşti paşi:

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



Introducere parolă

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

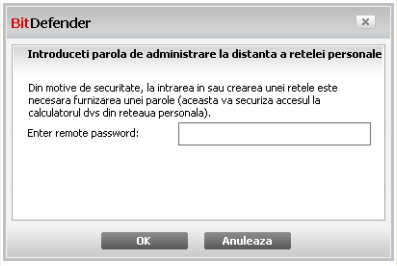


Adaugare calculator

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.



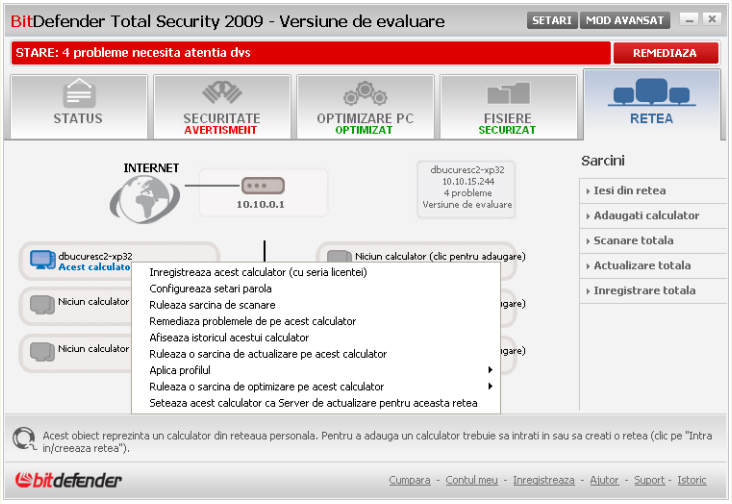
Autentificare

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.

9.1.3. Administrarea rețelei BitDefender

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



Hartă rețea

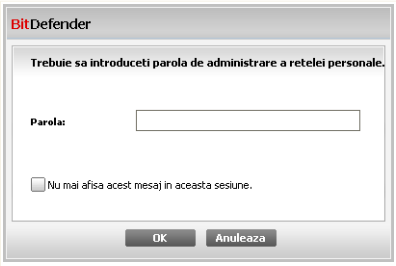
Dacă plasați cursorul mouse-ului deasupra unui calculator de pe harta rețelei, puteți vedea informații sumare despre acesta (nume, adresă IP, numărul de probleme care afectează securitatea sistemului, starea înregistrării).

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.

- **Înregistrează acest calculator**
- **Configurează parola pentru setări**
- **Execută o sarcină de scanare**
- **Repară probleme pe acest calculator**
- **Afişează evenimentele de pe acest calculator**
- **Execută o actualizare pe acest calculator acum**
- **Aplică profil**
- **Execută o sarcină de optimizare pe acest calculator**

■ **Setați acest calculator ca server de actualizare al acestei rețele**

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 şi faceți clic pe **OK**.

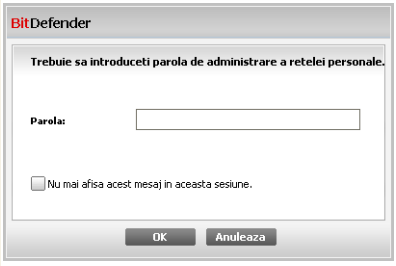
Notă

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.

9.1.4. Scanarea tuturor calculatoarelor

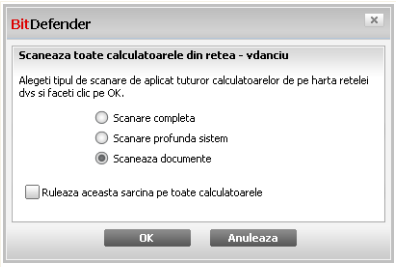
Pentru a scana toate calculatoarele administrate, urmați aceşti paşi:

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 completă sistem** - inițiază o scanare completă a calculatorului dumneavoastră (arhivele nu sunt scanate).
   - **Scanare completă sistem** - inițiază o scanare completă a calculatorului dumneavoastră (inclusiv arhivele).
   - **Scanează Documentele mele** - inițiază o scanare rapidă a documentelor şi setărilor dumneavoastră.



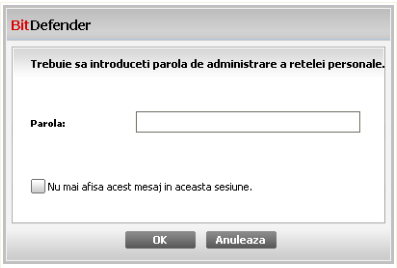
Selectați tipul de analiză.

3. Faceți clic pe **OK**.

9.1.5. Actualizarea tuturor calculatoarelor

Pentru a actualiza toate calculatoarele administrate, urmați aceşti paşi:

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



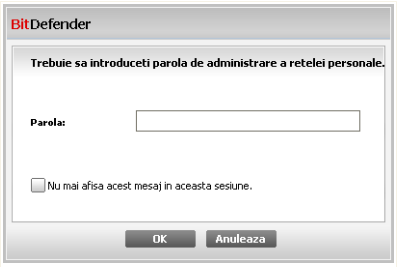
Introducere parolă

2. Faceți clic pe **OK**.

9.1.6. Înregistrarea tuturor calculatoarelor

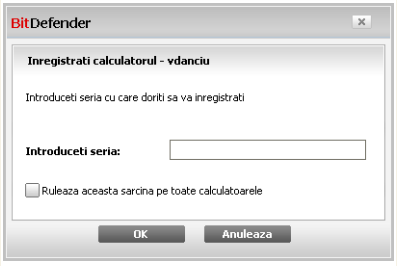
Pentru a înregistra toate calculatoarele administrate, urmați aceşti paşi:

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**.

10. Setări de bază

Modulul Setări de bază vă permite să activați sau să dezactivați cu uşurință module importante de securitate.

Pentru a accesa modulul Setări de bază, faceți clic pe butonul **Setări**, situat în partea de sus a modului de vizualizare de bază.

Setări de bază

Modulele de securitate disponibile sunt grupate în mai multe categorii.

Categorie	Descriere
Securitate locală	Aici puteți activa / dezactiva protecția în timp real sau actualizarea automată.
Securitate online	Aici puteți activa / dezactiva protecția în timp real pentru mesajele e-mail şi web.
Setări control parental	Aici puteți activa / dezactiva controlul parental.
Securitate rețea	Aici puteți activa / dezactiva firewallul.

Categorie	Descriere
Setări seif de fişiere	Aici puteți activa / dezactiva seiful de fişiere.
Setări generale	Aici puteți activa / dezactiva modul pentru jocuri, modul pentru laptop, parolele, bara de scanare şi alte opțiuni.

Faceți clic pe semnul “+” pentru a deschide o categorie sau pe “-” pentru a închide categoria.

10.1. Securitate locală

Puteți activa / dezactiva module de securitate cu un singur clic.

Modul securitate	Descriere
Protecție Antivirus & Antispyware pentru fişiere în timp real	Protecția în timp real scanarea tuturor fişierelor accesate de către dumneavoastră sau de către o aplicație care rulează pe acest sistem.
Actualizare automată	Actualizarea automată asigură descărcarea şi instalarea automată a celor mai recente fişiere de produs şi semnături BitDefender în mod regulat.
Verificare automată vulnerabilități	Verificarea automată a vulnerabilităților asigură menținerea la zi a aplicațiilor critice de pe calculatorul dumneavoastră.

10.2. Securitate online

Puteți activa / dezactiva module de securitate cu un singur clic.

Modul securitate	Descriere
Protecție Antivirus, Antispam & Antiphishing pentru e-mail în timp real	Protecția în timp real pentru mail asigură scanarea tuturor e-mailurilor pentru blocarea conținutului spam şi a tentativelor de phishing.

Modul securitate	Descriere
Protecție Antivirus & Antispyware pentru web în timp real	Protecția în timp real pentru web asigură scanarea după viruşi şi spyware a tuturor fişierelor descărcate de pe pagini web.
Protecție antiphishing în timp real pentru web	Protecția antiphishing în timp real pentru web asigură scanarea tuturor paginilor web pentru blocarea tentativelor de phishing.
Control identitate	Controlul identității vă ajută să păstrați în siguranță datele dumneavoastră confidențiale scanând tot traficul web şi e-mail după şiruri de caractere specifice.
Criptare IM	În cazul în care contactele dumneavoastră de IM au BitDefender 2009 instalat, toate conversațiile IM prin Yahoo! Messenger şi Windows Live Messenger vor fi criptate.

10.3. Setări control parental

Puteți activa / dezactiva modulul Control parental cu un singur clic.

Modulul Control parental poate bloca accesul la pagini web cu conținut inadecvat sau la Internet, pentru anumite perioade, şi poate filtra traficul e-mail, IM şi web după anumite cuvinte.

10.4. Setări rețea

Puteți activa / dezactiva modulul Firewall cu un singur clic.

Firewallul vă protejează calculatorul de atacurile din exterior ale hackerilor şi aplicațiilor periculoase.

10.5. Setări seif de fișiere

Puteți activa / dezactiva module Seif de fişiere cu un singur clic.

Seiful de fişiere păstrează confidențialitatea documentelor dumneavoastră criptându-le în seife speciale de fişiere.

10.6. Setări generale

Puteți activa / dezactiva elemente legate de securitate cu un singur clic.

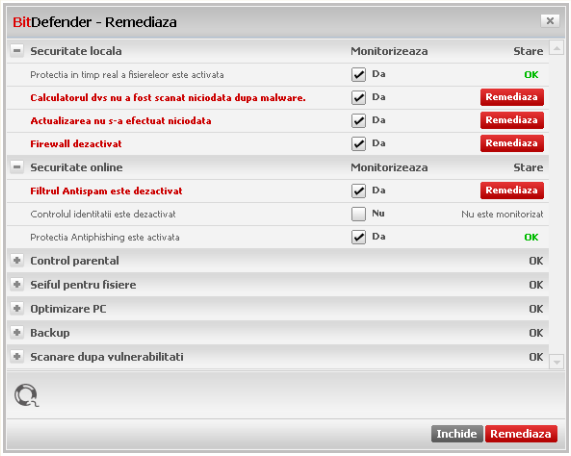
Element	Descriere
Mod pentru jocuri	Modul pentru jocuri modifică temporar setările de protecție pentru a minimiza impactul acestora asupra performanței sistemului atunci când vă jucați pe calculator.
Mod pentru laptop	Modul pentru laptop modifică temporar setările de protecție pentru a minimiza impactul 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.
Parolă control parental	Selectând această opțiune, veți limita protecția prin parolă doar la setările modulului Control parental. Aceasta asigură că setările controlului parental al BitDefender pot fi modificate doar de către persoanele care cunosc această parolă.
Ştiri BitDefender	Activând această opțiune, veți primi ştiri 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 bară mică, transparentă care indică progresul activității de scanare a BitDefender. Liniile verzi arată activitatea de scanare de pe sistemul dumneavoastră local. Liniile roşii arată activitatea de scanare a conexiunii dumneavoastră la Internet.
Încarcă BitDefender la pornirea Windows	Activând această opțiune, interfața BitDefender este încărcată la pornirea Windows. Această opțiune nu are nicio influență asupra nivelului de protecție.
Trimite rapoarte viruşi	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 şi nu vor fi folosite în scop comercial.

Element	Descriere
Detecție epidemii virale	Activând această opțiune, BitDefender va trimite rapoarte privind potențiale epidemii virale către Laboratorul BitDefender pentru analiză. Aceste rapoarte nu vor conține date confidențiale, cum ar fi numele dumneavoastră sau adresa IP, şi nu vor fi folosite în scop comercial.

11. Bara de stare

După cum uşor se poate observa, în partea superioară a ferestrei BitDefender Total Security 2009 există o bară de stare care afişează numărul de probleme existente. Faceți clic pe butonul **Repară tot** pentru a elimina rapid orice ameninţări la adresa securităţii calculatorului dumneavoastră. Va apărea o fereastră care indică situația securității sistemului.

Fereastra afişează o listă organizată sistematic şi uşor de gestionat a vulnerabilităților de securitate la care este expus calculatorul dumneavoastră. BitDefender Total Security 2009 vă va înştiința de fiecare dată când o problemă poate afecta securitatea calculatorului dumneavoastră.



Bara de stare

11.1. Securitate locală

Ştim că este important să fiți înştiințat ori de câte ori o problemă poate afecta securitatea calculatorului dumneavoastră. Prin monitorizarea fiecărui modul de securitate, BitDefender Total Security 2009 vă va înştiința nu numai atunci când configurați setări care ar putea afecta securitatea calculatorului dumneavoastră, ci şi atunci când uitați să executați sarcini importante.

Problemele privind securitatea locală sunt descrise în propoziții explicite. Dacă există probleme care ar putea afecta securitatea calculatorului dumneavoastră, veți vedea un buton roşu **Repară** în dreptul fiecăreia dintre acestea. Altfel, este afişat un buton verde **OK**.

Problemă	*Descriere*
Protecția în timp real este activată	Asigură scanarea tuturor fişierelor accesate de către dumneavoastră sau de către o aplicație care rulează pe acest sistem.
Ați scanat calculatorul după malware astăzi	Este recomandat să executați o scanare la cerere, cât mai curând posibil, pentru a verifica dacă fişierele stocate pe calculatorul dumneavoastră conțin malware.
Actualizarea automată este activată	Vă rugăm să mențineți activată actualizarea automată pentru a vă asigura că semnăturile de malware ale produsului dumneavoastră BitDefender sunt actualizate în mod regulat.
Actualizare în curs	Actualizarea produsului şi a semnăturilor de malware este în curs de desfăşurare.

Atunci când butoanele de stare au culoarea verde, sistemul dumneavoastră este în siguranță. Pentru a remedia potențialele probleme, urmați aceşti paşi:

1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

Dacă nu doriți ca o anumită problemă să fie monitorizată, debifați căsuța **Da, monitorizează această componentă**.

11.2. Securitate online

Problemele privind securitatea online sunt descrise în propoziții explicite. Dacă există probleme care ar putea afecta securitatea calculatorului dumneavoastră, veți vedea un buton roşu **Repară** în dreptul fiecăreia dintre acestea. Altfel, este afişat un buton verde **OK**.

Problemă	Descriere
Protecția în timp real pentru traficul web (HTTP) este activată	Este recomandat să mențineți protecția web (HTTP) activată pentru a vă proteja calculatorul împotriva aplicațiilor malițioase care se răspândesc prin intermediul site-urilor web şi împotriva fişierelor infectate descărcate.
Protecția în timp real pentru e-mailuri este activată	Protecția pentru traficul e-mail asigură că e-mailurile dumneavoastră sunt filtrate după malware şi conținut spam.
Protecția în timp real pentru traficul IM este activată	Este recomandat să activați protecția completă pentru traficul de mesagerie instant pentru a asigura securitatea calculatorului dumneavoastră.
Controlul identității este activat	Vă ajută să păstrați datele confidențiale în siguranță scanând tot traficul web şi mail după anumite stringuri. Este recomandat să activați Controlul identității pentru a împiedica furtul datelor dumneavoastră confidențiale (adresa de mail, parole, numere de carduri de credit etc).
Criptarea conversațiilor prin IM este activată	În cazul în care contactele dumneavoastră de IM au BitDefender 2009 instalat, toate conversațiile IM prin Yahoo! Messenger şi Windows Live Messenger vor fi criptate. Este recomandat să aveți activată criptarea IM pentru a vă asigura că discuțiile dumneavoastră prin mesageria instant rămân private.
Protecția antiphishing pentru Firefox este activată	BitDefender vă protejează împotriva tentativelor de phishing atunci când navigați pe Internet.
Protecția antiphishing pentru Internet Explorer este activată	BitDefender vă protejează împotriva tentativelor de phishing atunci când navigați pe Internet.

Atunci când butoanele de stare au culoarea verde, sistemul dumneavoastră este în siguranță. Pentru a remedia potențialele probleme, urmați aceşti paşi:

1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

Dacă nu doriți ca o anumită problemă să fie monitorizată, debifați căsuța **Da, monitorizează această componentă**.

11.3. Securitate rețea

Atunci când calculatorul dumneavoastră face parte dintr-o rețea, doriți cu siguranță ca acesta să fie protejat împotriva hackerilor şi să fie blocate orice conexiuni neautorizate.

Problemele privind securitatea rețelei sunt descrise în propoziții explicite. Dacă există probleme care ar putea afecta securitatea calculatorului dumneavoastră, veți vedea un buton roşu **Repară** în dreptul fiecăreia dintre acestea. Altfel, este afişat un buton verde **OK**.

Problemă	*Descriere*
Firewallul este activat	Vă protejează calculatorul de atacurile din exterior ale hackerilor şi aplicațiilor periculoase.

Atunci când butoanele de stare au culoarea verde, sistemul dumneavoastră este în siguranță. Pentru a remedia potențialele probleme, urmați aceşti paşi:

1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

Dacă nu doriți ca o anumită problemă să fie monitorizată, debifați căsuța **Da, monitorizează această componentă**.

11.4. Control parental

Controlul parental monitorizează starea modulelor care vă permit să restricționați accesul copiilor dumneavoastră la Internet şi la anumite aplicații.

Problemele privind modulul de control parental sunt descrise în propoziții explicite. Dacă există ceva care ar putea afecta copiii dumneavoastră, veți vedea un buton roşu **Repară** în dreptul fiecărei probleme. Altfel, este afişat un buton verde **OK**.

Problemă	Descriere
Controlul parental nu este configurat	Modulul Control parental poate bloca accesul la pagini web cu conținut inadecvat, poate bloca accesul la Internet pentru anumite perioade şi poate filtra traficul mail, IM şi web după anumite cuvinte etc.

Atunci când butoanele de stare au culoarea verde, copiii dumneavoastră pot naviga în siguranță pe web. Pentru a remedia potențialele probleme, urmați aceşti paşi:

1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

Dacă nu doriți ca o anumită problemă să fie monitorizată, debifați căsuța **Da, monitorizează această componentă**.

11.5. Seif de fișiere

Problemele privind confidențialitatea datelor dumneavoastră sunt descrise în propoziții explicite. Dacă există astfel de probleme, veți vedea un buton roşu **Repară** în dreptul fiecăreia dintre acestea. Altfel, este afişat un buton verde **OK**.

Problemă	Descriere
Seiful de fişiere este activat	Seiful de fişiere păstrează confidențialitatea documentelor dumneavoastră criptându-le în seife speciale de fişiere.

Atunci când butoanele de stare au culoarea verde, datele dumneavoastră sunt în siguranță. Pentru a remedia potențialele probleme, urmați aceşti paşi:

1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

Dacă nu doriți ca o anumită problemă să fie monitorizată, debifați căsuța **Da, monitorizează această componentă**.

11.6. Optimizare

Problemele care ar putea afecta performanța calculatorului dumneavoastră sunt descrise în propoziții explicite. Dacă există astfel de probleme, veți vedea un buton roşu **Repară** în dreptul fiecăreia dintre acestea. Altfel, este afişat un buton verde **OK**.

Problemă	*Descriere*
Nu ați curățat niciodată regiştrii	Asistentul de curățare a regiştrilor scanează regiştrii Windows şi şterge cheile de regiştri nevalide. Curățați regiştrii periodic pentru a creşte performanțele sistemului dumneavoastră.
Nu ați curățat niciodată calculatorul	Curățarea periodică a calculatorului îmbunătățeşte performanțele acestuia. Executați această sarcină cât mai curând posibil.
Nu ați căutat niciodată fişiere duplicate	Asistentul de căutare a fişierelor duplicate optimizează spațiul pe disc descoperind fişierele duplicate de pe sistemul dumneavoastră. Urmați acest asistent cât mai curând posibil.
Nu ați defragmentat niciodată hard discul	Asistentul de defragmentare a discului reorganizează datele de pe hard-disc la nivel fizic astfel încât bucățile care compun fiecare fişier să fie stocate cât mai aproape şi în mod continuu. Defragmentați hard-discul cât mai curând posibil.

Atunci când butoanele de stare au culoarea verde, sistemul dumneavoastră este în siguranță. Pentru a remedia potențialele probleme, urmați aceşti paşi:

1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

Dacă nu doriți ca o anumită problemă să fie monitorizată, debifați căsuța **Da, monitorizează această componentă**.

11.7. Backup

Problemele care ar putea afecta siguranța datelor dumneavoastră sunt descrise în propoziții explicite. Dacă există astfel de probleme, veți vedea un buton roşu **Repară** în dreptul fiecăreia dintre acestea. Altfel, este afişat un buton verde **OK**.

Problemă	Descriere
Ați executat o sarcină de backup local pe calculatorul dumneavoastră cu x zile în urmă	Modulul de backup local vă ajută să faceți copii de rezervă pentru orice date importante de pe sistemul dumneavoastră.

Atunci când butoanele de stare au culoarea verde, datele dumneavoastră sunt în siguranță. Pentru a remedia potențialele probleme, urmați aceşti paşi:

1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

Dacă nu doriți ca o anumită problemă să fie monitorizată, debifați căsuța **Da, monitorizează această componentă**.

11.8. Căutare vulnerabilități

Problemele privind vulnerabilitățile sistemului sunt descrise în propoziții explicite. Dacă există probleme care ar putea afecta securitatea calculatorului dumneavoastră, veți vedea un buton roşu **Repară** în dreptul fiecăreia dintre acestea. Altfel, este afişat un buton verde **OK**.

Problemă	Descriere
Căutarea de vulnerabilități este activată	Monitorizează sistemul de actualizare al Microsoft Windows şi al Microsoft Windows Office şi parolele conturilor Microsoft Windows pentru a vă asigura că sistemul dumneavoastră de operare este actualizat şi că parolele nu pot fi ghicite uşor.
Actualizări Microsoft critice	Instalează actualizările critice disponibile de la Microsoft.
Alte actualizări Microsoft	Instalează actualizările normale disponibile de la Microsoft.
Windows Automatic Updates este activat	Instalează noile actualizări de securitate pentru Windows imediat ce acestea sunt disponibile.

Problemă	Descriere
Administrator (parolă puternică)	Indică siguranța pe care o oferă parola configurată pentru un anumit utilizator (cât de uşor poate fi ghicită).

Atunci când butoanele de stare au culoarea verde, sistemul dumneavoastră este în siguranță. Pentru a remedia potențialele probleme, urmați aceşti paşi:

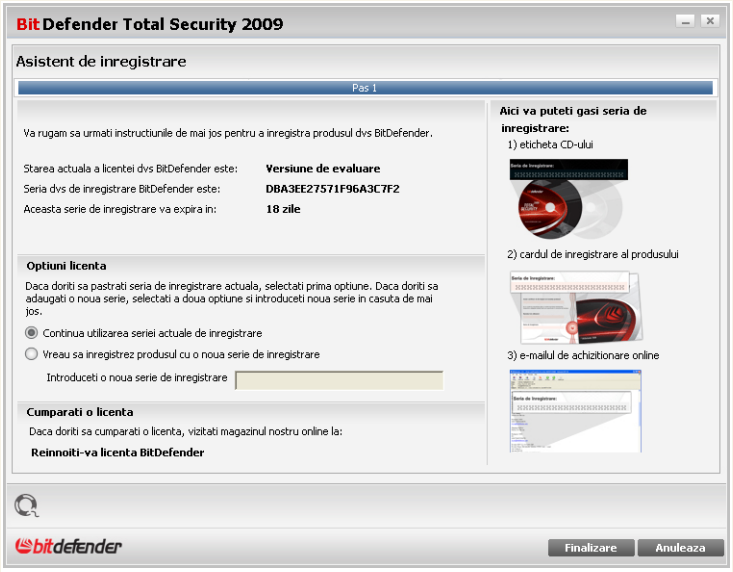
1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

Dacă nu doriți ca o anumită problemă să fie monitorizată, debifați căsuța **Da, monitorizează această componentă**.

12. Înregistrare

Perioada de evaluare a BitDefender Total Security 2009 este de 30 de zile. Dacă doriți să înregistrați BitDefender Total Security 2009, să schimbați seria de înregistrare sau să creați un cont BitDefender, faceți clic pe linkul **Înregistrează**, situat în partea de jos a ferestrei BitDefender. Va apărea asistentul de înregistrare.

12.1. Pasul 1/1 - Înregistrați BitDefender Total Security 2009



Înregistrare

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

Dacă perioada de evaluare nu a expirat şi doriți să evaluați produsul în continuare, selectați **Continuă evaluarea produsului**.

Pentru a înregistra BitDefender Total Security 2009:

1. Selectați **Vreau să înregistrez produsul cu o nouă serie**.
2. Introduceți seria de înregistrare în câmpul editabil.

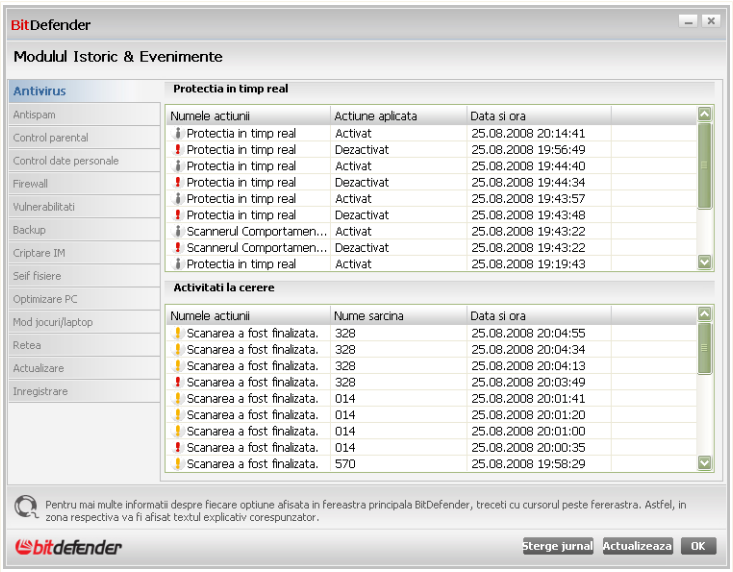
Notă
Puteți găsi seria dumneavoastră de înregistrare:
- pe eticheta de pe CD.
- pe certificatul de înregistrare al produsului.
- în e-mailul de achiziționare online.

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

Faceți clic pe **Finalizare**.

13. Istoric

Linkul **Istoric**, situat în partea de jos a ferestrei BitDefender, deschide o nouă fereastră conținând istoricul şi evenimentele BitDefender. Această fereastră vă furnizează un sumar al evenimentelor legate de securitate. De exemplu, puteți verifica rapid dacă produsul a fost actualizat, dacă au fost detectate aplicații malițioase pe calculatorul dumneavoastră, dacă sarcinile de backup au rulat fără erori etc.



Evenimente

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

- **Antivirus**
- **Firewall**
- **Antispam**
- **Control date**
- **Control parental**

- **Actualizare**
- **Întreținere PC**
- **Backup**
- **Rețea**
- **Criptare IM**
- **Seif de fişiere**

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 şi data şi 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 **Şterge jurnal** dacă doriți să ştergeți rapoartele vechi sau pe **Actualizare** pentru a vă asigura că şi ultimele evenimente sunt afişate.

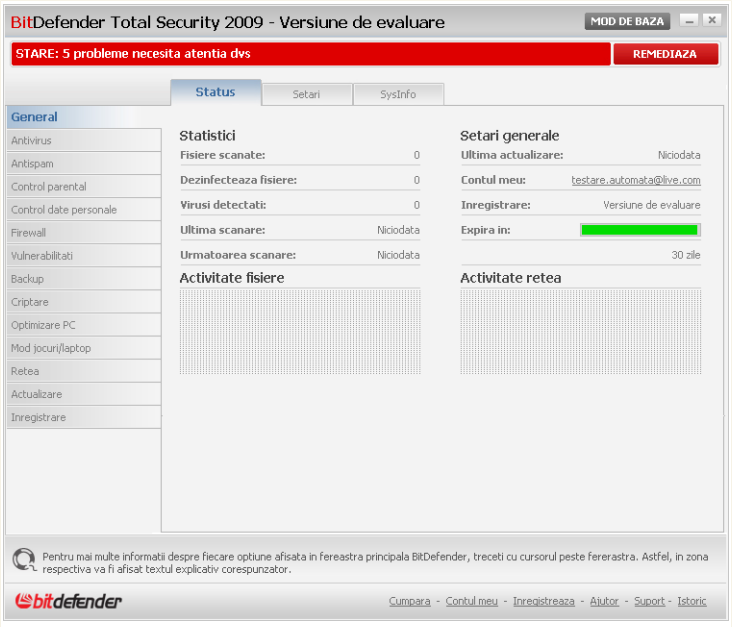
Administrare avansată

14. General

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

14.1. Pagina de gardă

Pentru a vedea statistici despre activitatea produsului şi situația înregistrării, mergeți la **General>Sumar** în modul avansat.



Pagina de gardă

Pagina de gardă conține mai multe secțiuni:

- **Statistici** - Afişează informații importante referitoare la activitatea BitDefender.

- **Prezentare generală** - Afişează informaţii referitoare la actualizare, contul dumneavoastră, înregistrare şi licenţă.
- **Zonă fişiere** - Indică evolutia numărului de obiecte scanate de către BitDefender Antimalware. Înălţimea barelor indică intensitatea traficului în intervalul de timp respectiv.
- **Zonă reţea** - Indică evolutia traficului de reţea filtrat de către firewallul BitDefender. Înălţimea barelor indică intensitatea traficului în intervalul de timp respectiv.

14.1.1. Statistici

Dacă doriţi să urmăriţi activitatea BitDefender, puteţi începe cu secţiunea Statistici. Următoarele elemente sunt afişate:

Element	Descriere
Fişiere scanate	Indică numărul de fişiere care au fost verificate după malware la ultima scanare.
Fişiere dezinfectate	Indică numărul de fişiere care au fost dezinfectate la ultima scanare.
Viruşi detectaţi	Indică numărul viruşilor detectaţi în sistemul dumneavoastră la ultima scanare.
Scanări de porturi blocate	Indică numărul de scanări de porturi blocate de firewallul BitDefender. Scanările de porturi sunt folosite în mod frecvent de hackeri pentru a detecta porturi deschise pe calculatorul dumneavoastră cu intenţia de a le exploata. Menţineţi firewallul şi modul ascuns activate pentru a fi protejat împotriva scanărilor de porturi.
Sarcini de backup finalizate	Indică de câte ori aţi făcut copii de siguranţă pentru fişierele dumneavoastră.

14.1.2. Descriere generală

Aici puteti vedea un sumar al statisticilor cu privire la actualizare, contul dumneavoastră, înregistrare şi licenţă.

Element	Descriere
Ultima actualizare	Indică data la care produsul dumneavoastră BitDefender a fost actualizat ultima oară. Vă rugăm să efectuați actualizări în mod regulat, pentru a avea un sistem complet protejat.
Contul meu	Indică adresa de e-mail pe care o puteți utiliza pentru a vă accesa contul online, unde vă puteți recupera seria de înregistrare pierdută şi puteți beneficia de suport BitDefender si alte servicii personalizate.
Înregistrare	Indică tipul şi 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.

14.2. Setări

Pentru a configura setările generale ale BitDefender şi pentru a administra setările, faceți clic pe **General>Setări** în modul avansat.

Setări generale

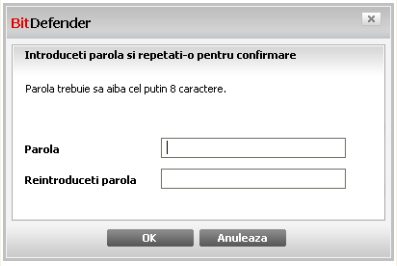
Aici puteți seta comportamentul general al produsului. BitDefender se încarcă la pornirea Windows iar apoi rulează minimizat în bara de sistem.

14.2.1. 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 foloseşte 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** şi 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 şi opțiunea **Cere/Aplică parola doar pentru Controlul parental**. Pe de altă parte, dacă parola a fost configurată doar pentru Controlul parental şi 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.
- **Afişează ştiri BitDefender (avertizări de securitate)** - afişează din când în când notificări de securitate referitoare la noi viruşi descoperiți, trimise de serverul BitDefender.
- **Afişează ferestre pop-up (note pe ecran)** - afişează ferestre de informare cu privire la starea produsului.
- **Încarcă BitDefender la pornirea Windows** - lansează BitDefender automat, la pornirea sistemului de operare. Această opțiune este recomandată.
- **Afişează bara de scanare (graficul de pe ecran al activității produsului)** - afişează bara de scanare atunci când vă conectați la Windows. Debifați această căsuță dacă nu doriți ca bara de scanare să mai fie afişată.

Notă
Această opțiune poate fi configurată doar pentru contul de utilizator Windows curent.

14.2.2. Setări raportare viruși

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

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

14.3. Informații sistem

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

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

Informații sistem

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

Sunt disponibile trei butoane:

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

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

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

15. Antivirus

BitDefender vă protejează calculatorul împotriva oricăror ameninţări malitioase (viruşi, troieni, aplicaţii spyware, rootkituri şi altele). Protecţia oferită de BitDefender se împarte în două categorii:

- Protecţia în timp real - previne pătrunderea noilor ameninţări malware în sistemul dumneavoastră. BitDefender va scana, de exemplu, un document Word atunci când îl deschideţi şi un mesaj e-mail atunci când îl primiţi.

  Notă
  Protecţia în timp real mai este denumită şi scanare la acces - fişierele sunt scanate în timp ce utilizatorii le accesează.

- Scanarea la cerere - permite detectarea şi ştergerea aplicaţiilor malitioase care există deja în sistemul dumneavoastră. Acesta este modul clasic de scanare, iniţiată de utilizator – dumneavoastră alegeţi partiţiile, directoarele sau fişierele pe care trebuie să le scaneze BitDefender, iar BitDefender le scanează – la cerere. Sarcinile de scanare permit crearea unor rutine de scanare personalizate şi pot fi programate să ruleze periodic.

15.1. Protecţie în timp real

BitDefender oferă protecţie continuă în timp real împotriva unui număr mare de ameninţări malitioase scanând toate fişierele accesate, mesajele e-mail şi comunicaţiile prin programe de mesagerie instantă (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). BitDefender Antiphishing împiedică dezvăluirea informaţiilor personale în timp ce navigaţi pe Internet alertându-vă despre paginile web cu conţinut potenţial phishing.

Pentru a configura protecţia în timp real şi BitDefender Antiphishing, mergeţi la **Antivirus>Scut** în modul avansat.

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 viruşi, păstrați **Protectia in timp real** activată.

Pentru a iniția o scanare rapidă a sistemului, faceți clic pe **Scanează acum**.

15.1.1. 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:

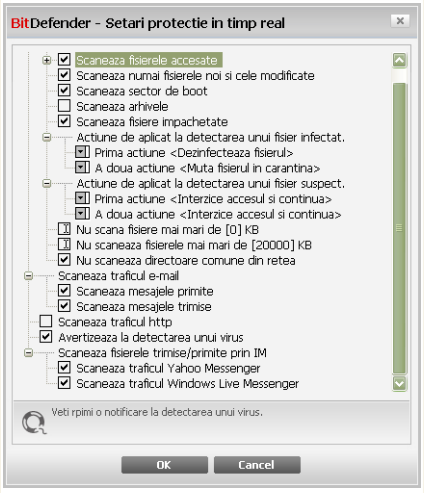
Nivel de protecţie	Descriere
Permisiv	Acoperă nevoile elementare de securitate. Consumul de resurse este foarte scăzut. Aplicaţiile şi mesajele e-mail primite sunt scanate doar împotriva viruşilor. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică. Acţiunile luate asupra fişierelor infectate sunt următoarele: dezinfectează fişier/interzice accesul.
Standard	Oferă protecţie standard. Consumul de resurse este scăzut. Toate fişierele şi mesajele e-mail sunt scanate împotriva viruşilor şi a aplicaţiilor. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică. Acţiunile luate asupra fişierelor infectate sunt următoarele: dezinfectează fişier/interzice accesul.
Agresiv	Oferă protecţie avansată. Consumul de resurse este moderat. Toate fişierele şi mesajele e-mail, precum şi traficul web, sunt scanate împotriva viruşilor şi a aplicaţiilor. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică. Acţiunile luate asupra fişierelor infectate sunt următoarele: dezinfectează fişier/interzice accesul.

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

15.1.2. Personalizarea nivelului de protecţie

Utilizatorii avansaţi pot folosi şi modifica opţiunile de scanare oferite de BitDefender în beneficiul lor. Motorul de scanare poate fi setat să scaneze doar anumite extensii de fişiere, să caute anumite tipuri de ameninţări malitioase sau să nu scaneze arhivele. Aceasta poate reduce cu mult timpul de scanare, precum şi viteza de reacţie a sistemului pe durata scanării.

Puteţi personaliza **Protecţia în timp real** făcând 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, deşi 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, ele vor putea fi deschise.

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

Opțiune		*Descriere*
Scanează fişiere accesate	**Scanează toate fisierele**	Vor fi scanate toate fişierele accesate, indiferent de tipul lor.
	Programe	Nu vor fi scanate decât fişierele program, şi anume fişierele cu următoarele extensii: `.exe`;

Opțiune		Descriere
		.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 şi .nws.
	Extensiile definite de utilizator	Nu vor fi scanate decât fişierele cu extensiile specificate de utilizator. Aceste extensii trebuie separate prin ";".
	Scanează după soft cu risc	Scanează după aplicații care prezintă un potențial risc (riskware). Fişierele detectate vor considerate ca fiind infectate. Programele care includ componente adware se pot opri din funcționare dacă această opțiune este activată. Selectați **Nu scana aplicații si programe dialer** dacă doriți să excludeți aceste fişiere de la scanare.
Scanează boot		Scanează sectorul de boot al sistemului.
Deschide arhive		Vor fi scanate şi arhivele accesate. Selectând această opțiune, performanțele calculatorului vor scădea.
Deschide programele împachetate		Programele împachetate accesate vor fi scanate.
Prima acțiune		Selectați din meniu prima acțiune ce va fi luată asupra fişierelor infectate sau suspecte.
	Interzice accesul şi continuă	În caz că un fişier este infectat, accesul la acesta va fi interzis.
	Dezinfectează fişier	Dezinfectează fişierele infectate.

Opțiune		Descriere
	Şterge fişier	Şterge imediat fişierele infectate, fără niciun avertisment.
	Mută fişier în carantină	Mută fişierele infectate în carantină.
A doua acțiune		Selectați din meniu a doua acțiune pentru fişierele infectate sau suspecte, în caz că prima acțiune eşuează.
	Interzice accesul şi continuă	În caz că un fişier este infectat, accesul la acesta va fi interzis.
	Şterge fişier	Şterge imediat fişierele infectate, fără niciun avertisment.
	Mută fişier în carantină	Mută fişierele infectate în carantină.
Nu scana fişiere mai mari de [x] Kb		Introduceți dimensiunea maximă a fişierelor ce vor fi scanate. Dacă dimensiunea este de 0 Kb, toate fişierele vor fi scanate, indiferent de mărimea lor.
Nu scana arhive mai mari de [20000] Kb		Introduceți dimensiunea maximă a arhivelor ce vor fi scanate, exprimată în kiloocteți (KB). Pentru a scana toate arhivele, indiferent de dimensiunea acestora, introduceți cifra 0.
Nu scana fişierele din rețea		Dacă această opțiune este activată, BitDefender nu va scana fişierele comune din rețea, permițând accesarea mai rapidă a acestora. Vă recomandăm să activați această opțiune doar dacă rețeaua din care faceți parte este protejată de o soluție antivirus.

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

  Următoarele opțiuni sunt disponibile:

Opțiune	Descriere
Scanează mesajele primite	Scanează toate mesajele primite.
Scanează mesajele trimise	Scanează toate mesajele trimise.

- **Scanează traficul http** - scanează tot traficul web.
- **Avertizează când este detectat un virus** - afişează o fereastră de avertizare la descoperirea unui virus într-un fişier sau mesaj e-mail.

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

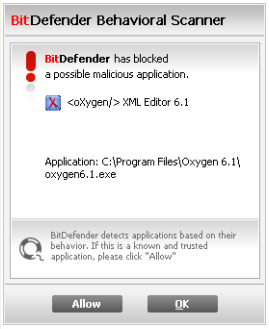
  Dacă este detectat un fişier suspect, din fereastra de alertă puteți lansa un program asistent ce vă va ajuta să trimiteți acest fişier Laboratorului BitDefender pentru analiză aprofundată. Pentru a primi informații despre acest fişier introduceți adresa dumneavoastră de e-mail.
- **Scanează fişierele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

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

15.1.3. Configurarea motorului de scanare comportamental

Motorul de scanare comportamental vă protejează împotriva amenințărilor noi, pentru care încă nu au fost lansate semnături. Acesta monitorizează şi analizează în mod constant comportamentul aplicațiilor care rulează pe calculatorul dumneavoastră şi vă alertează dacă o aplicație are un comportament suspicios.

Motorul de scanare comportamental vă alertează de fiecare dată când o aplicație încearcă să execute o acțiune potențial malițioasă şi vă cere să luați o acțiune.

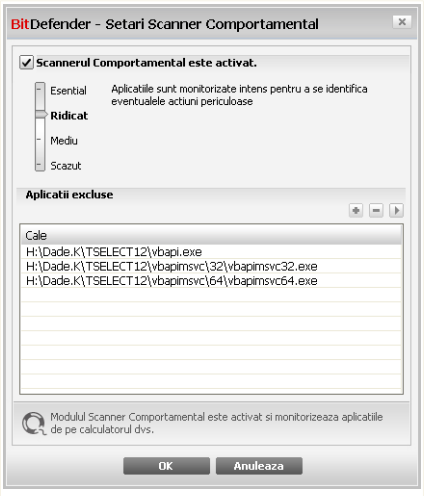


Alertă motor de scanare comportamental

Dacă aplicația detectată este cunoscută, faceți clic pe **Permite**. Motorul de scanare comportamental nu va mai scana aplicația în căutare de comportament potențial malițios.

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

Pentru a configura motorul de scanare comportamental, faceți clic pe **Setări scaner**.



Setări motor de scanare comportamental

Dacă doriți să dezactivați motorul de scanare comportamental, debifați căsuța **Motorul de scanare comportamental este activat**.

Important
Mențineți motorul de scanare comportamental activat pentru a vă proteja împotriva viruşilor necunoscuți.

Configurarea nivelului de protecție

Nivelul de protecție al motorului de scanare comportamental este modificat automat atunci când setați un nou nivel al protecției în timp real. Dacă nu vă mulțumeşte setarea implicită, puteți configura manual nivelul de protecție.

Notã
Țineți minte că, dacă schimbați nivelul protecției în timp real, se va modifica în consecință şi nivelul protecției motorului de scanare comportamental.

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

Nivel de protecție	*Descriere*
Critic	Aplicațiile sunt monitorizate strict pentru identificarea unor potențiale acțiuni malițioase.
Ridicat	Aplicațiile sunt monitorizate intens pentru identificarea unor potențiale acțiuni malițioase.
Mediu	Aplicațiile sunt monitorizate moderat pentru identificarea unor potențiale acțiuni malițioase.
Scăzut	Aplicațiile sunt monitorizate pentru identificarea unor potențiale acțiuni malițioase.

Administrarea aplicațiilor excluse

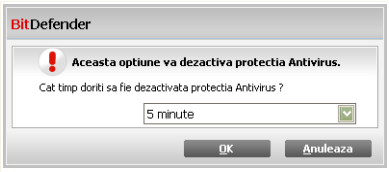
Puteți configura motorul comportamental de scanare să nu verifice anumite aplicații. Pentru a activa această protecție selectați căsuța corespunzătoare opțiunii **Activează controlul aplicațiilor**.

Pentru administrarea aplicațiilor excluse, puteți utiliza butoanele situate în partea de sus a tabelului:

- **Add** - exclude a new application from scanning.
- **Remove** - remove an application from the list.
- **Edit** - edit an application path.

15.1.4. Dezactivarea protecției în timp real

Dacă doriți să dezactivați protecția în timp real, va apărea o fereastră de avertizare.



Dezactivați protecția în timp real

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.

15.1.5. 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 şi 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 la lista albă, introduceți adresa acestuia în câmpul **Adresă nouă** şi 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.

Notã

Puteți adăuga uşor site-uri web la lista albă din bara de comenzi BitDefender Antiphishing integrată în browserul dumneavoastră.

Pentru a şterge un site din lista albă, faceți clic pe butonul **Şterge** corespunzător.

Faceți clic pe **Închide** pentru a salva modificările şi închide fereastra.

15.2. Scanarea la cerere

Principalul obiectiv BitDefender este protejarea calculatorului dumneavoastră de viruşi. Aceasta se face în primul rând nepermițând viruşilor noi să pătrundă în sistem, prin scanarea mesajelor e-mail şi a fişierelor 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 viruşi după instalarea BitDefender. Şi este, de asemenea, recomandat să vă scanați sistemul periodic.

Pentru a configura şi iniția scanarea la cerere, mergeți la **Antivirus>Scanare** în modul avansat.

Sarcini de scanare

Scanarea la cerere se bazează pe sarcini de scanare. Sarcinile de scanare sunt cele care specifică opțiunile de scanare şi 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.

15.2.1. 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.

Fiecare sarcină are propria fereastră de **Proprietăți** care permite configurarea sarcinii şi examinarea rezultatelor scanării. Pentru mai multe informații, consultați "*Configurarea sarcinilor de scanare*" (p. 188).

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 viruşii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) şi altele.
Scanare completă sistem	Scanează întregul sistem, cu excepția arhivelor. În configurația implicită, se scanează după toate tipurile de aplicații malițioase care amenință securitatea sistemului dumneavoastră, cum ar fi viruşii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) şi altele.
Scanare rapidă sistem	Scanează directoarele `Windows`, `Program Files` şi `All Users`. În configurația implicită, se scanează după toate tipurile de aplicații malițioase, mai puțin cele ascunse (rootkituri), dar nu sunt scanate memoria, regiştrii şi fişierele cookie.
Scanare automată la conectare	Scanează obiectele executate atunci când un utilizator se conectează la Windows. În mod implicit, scanarea automată la conectare porneşte la 3 minute după ce utilizatorul s-a conectat.

Notă
Deoarece sarcinile **Scanare profundă sistem** şi **Scanare completă sistem** analizează întregul sistem, scanarea poate lua ceva timp. De aceea, vă recomandăm să rulați aceste sarcini cu prioritate scăzută sau, şi mai bine, 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` şi `StartUp`. Astfel, veți asigura siguranța documentelor dumneavostră, un spațiu de lucru sigur şi 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 şi să examinați rapoartele de scanare.

În partea dreaptă a fiecărei sarcini sunt disponibile trei butoane:

- **Program** - indică faptul că sarcina selectată este planificată să ruleze mai tarziu. Faceți clic pe acest buton pentru a deschide fereastra de **Proprietăți** la tabul Planificare, unde puteți vedea şi modifica programul de rulare a sarcinii.
- **Şterge** - şterge sarcina selectată.

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

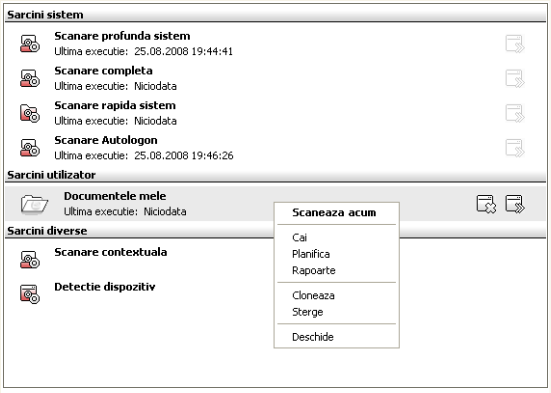
- **Scanare** - execută sarcina selectată, pornind o scanare imediată.

În partea stângă a fiecărei sarcini, puteți vedea butonul **Proprietăți** care vă permite să configurați sarcina şi să vedeți rapoartele de scanare.

15.2.2. Utilizarea meniului contextual

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

Următoarele opțiuni sunt disponibile pe meniul contextual:



Meniu contextual

- **Scanare** - rulează sarcina selectată, lansând o scanare imediată.
- **Schimbare cale** - deschide fereastra de **Proprietăți** la tabul Țintă, unde puteți modifica locațiile de scanare pentru sarcina selectată.

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

- **Planificare sarcină** - deschide fereastra de **Proprietăți** la tabul Planificare, unde puteți programa sarcina selectată.
- **Examinare rapoarte** - deschide fereastra de **Proprietăți** la tabul Rapoarte, unde puteți examina rapoartele generate de fiecare dată când sarcina selectată a rulat.
- **Duplicare** - creează o copie a sarcinii selectate.

Notă
Acest lucru este util în crearea de noi sarcini, deoarece puteți modifica setările duplicatului unei sarcini.

- **Şterge** - şterge sarcina selectată.

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

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

Notă
Datorită caracterului special al sarcinilor din categoria **Sarcini diverse**, doar opțiunile **Proprietăți** şi **Examinare rapoarte** sunt disponibile în acest caz.

15.2.3. Crearea sarcinilor de scanare

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

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

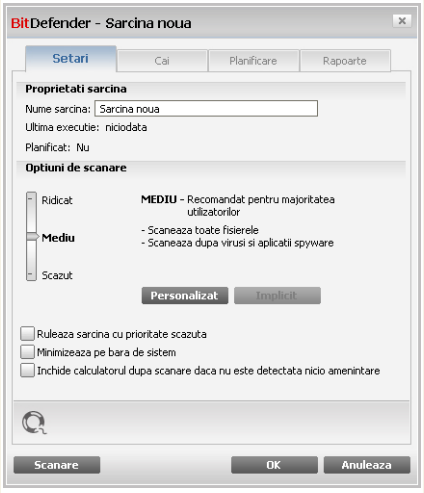
15.2.4. Configurarea sarcinilor de scanare

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 **Deschide**, situat în partea dreapta a sarcinii de scanare (sau faceți clic-dreapta pe sarcină şi apoi faceți clic pe **Deschide**).

Notă
Pentru mai multe informații despre vizualizarea rapoartelor şi tabul **Rapoarte**, consultați "*Examinarea rapoartelor de scanare*" (p. 208).

Configurarea setărilor de scanare

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



Descriere generală

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

Alegerea nivelului de scanare

Puteți configura uşor 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*
Scăzut	Oferă o rată de detecție moderată. Consumul de resurse este scăzut. Doar programele sunt scanate împotriva viruşilor. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică.
Mediu	Oferă o rată de detecție bună. Consumul de resurse este moderat.

Nivel de protecţie	Descriere
	Toate aplicaţiile sunt scanate împotriva viruşilor şi a aplicaţiilor spyware. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică.
Ridicat	Oferă o rată de detecţie ridicată. Consumul de resurse este şi el ridicat. Toate aplicaţiile şi arhivele sunt scanate împotriva viruşilor şi a aplicaţiilor spyware. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică.

Sunt de asemenea disponibile şi o serie de opţiuni generale privind procesul de scanare:

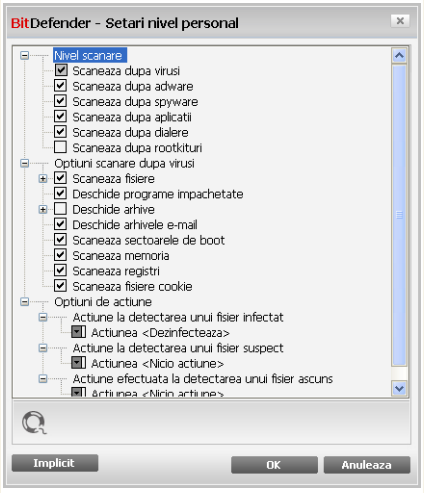
- **Rulează sarcina cu prioritate scăzută.** Reduce prioritatea procesului de scanare. Veţi permite altor programe să ruleze cu o viteză superioară, dar timpul necesar pentru finalizarea scanării va creşte.
- **Minimizează fereastra de scanare la bara de scanare.** Minimizează fereastra de scanare bara de sistem. Faceţi dublu-clic pe simbolul BitDefender pentru a o deschide.
- **Închide calculatorul la finalizarea scanării dacă nu este detectată nicio ameninţare**

Faceţi clic pe **OK** pentru a salva modificările şi închide fereastra. Pentru a executa sarcina faceţi clic pe **Scanează**.

Personalizarea nivelului de scanare

Utilizatorii avansaţi pot folosi şi modifica opţiunile de scanare oferite de BitDefender în beneficiul lor. Motorul de scanare poate fi setat să scaneze doar anumite extensii de fişiere, să caute anumite tipuri de ameninţări malitioase sau să nu scaneze arhivele. Aceasta poate reduce cu mult timpul de scanare, precum şi viteza de reacţie a sistemului pe durata scanării.

Faceţi clic pe **Personalizat** pentru a vă seta propriile opţiuni 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 viruşi	Scanează după viruşi cunoscuți. BitDefender detectează, de asemenea, şi corpurile incomplete de viruşi, îndepărtând astfel orice posibilă amenințare ce ar putea afecta securitatea sistemului dumneavoastră.
Scanează după adware	Scanează după amenințări adware. Fişierele detectate vor fi considerate ca fiind infectate. Programele care

Opțiune	Descriere
	includ componente adware se pot opri din funcționare dacă această opțiune este activată.
Scanează după spyware	Scanează după amenințări spyware cunoscute. Fişierele detectate vor fi considerate ca fiind infectate.
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. Fişierele 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 (fişiere şi procese), cunoscute sub denumirea generică de rootkituri.

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

Opțiune		Descriere
Scanează fişiere	**Scanează toate fisierele**	Toate fişierele sunt scanate, indiferent de tipul lor.
	Programe	Nu vor fi scanate decât fişierele program, şi anume fişierele 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` şi `nws`.

Opțiune		Descriere
	Extensiile definite de utilizator	Nu vor fi scanate decât fişierele cu extensiile specificate de utilizator. Aceste extensii trebuie separate prin ";".
Deschide programe impachetate		Scanează programele împachetate.
Deschide arhive		Scanează în interiorul arhivelor. Scanarea fişierelor arhivate necesită mai mult timp şi mai multe resurse de sistem. Puteți faceți clic pe câmpul **Dimensiunea limită a arhivelor** şi introduce dimensiunea maximă a arhivelor ce vor fi scanate, exprimată în kiloocteți (KB).
Deschide e-mail		Scanează în interiorul arhivelor de e-mail.
Scanează sectorul de boot		Scanează sectorul de boot al sistemului.
Scanare memorie		Scanează memoria împotriva viruşilor şi a altor aplicații malițioase.
Scanează regiştri		Scanează intrările din regiştri.
Scanează fişiere cookie		Scanează fişierele cookie.

- **Optiuni de acțiune .** Specificați acțiunea care trebuie aplicată fiecărei categorii de fişiere detectate utilizând opțiunile din categoria **Opțiuni de acțiune**.

Notă
Pentru a seta o nouă acțiune, faceți clic pe acțiunea curentă şi selectați opțiunea dorită din meniu.

- Selectați acțiunea ce trebuie aplicată fişierelor infectate detectate. Următoarele opțiuni sunt disponibile:

Acțiune	Descriere
Niciuna (înregistrează obiecte)	Nici se va efectua nicio acțiune în legătură cu fişierelor infectate. Aceste fişiere vor apărea în fişierul de raport.
Dezinfectează	Elimină codul malware din fişierele infectate detectate.

Acţiune	Descriere
Şterge	Şterge imediat fişierele infectate, fără niciun avertisment.
Mută în carantină	Mută fişierele infectate în carantină. Fişierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.

- Selectați acțiunea ce trebuie aplicată fişierelor detectate ca fiind infectate. Următoarele opțiuni sunt disponibile:

Acţiune	Descriere
Niciuna (înregistrează obiecte)	Nicio acțiune nu va fi aplicată fişierelor suspecte. Aceste fişiere vor apărea în fişierul de raport.
Şterge	Şterge imediat fişierele suspecte, fără niciun avertisment.
Mută în carantină	Mută fişierele suspecte în carantină. Fişierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.

Notă
Fişierele pot fi detectate ca fiind suspecte în urma analizei euristice. Vă recomandăm să trimiteți aceste fişiere Laboratorului BitDefender.

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

Acţiune	Descriere
Niciuna (înregistrează obiecte)	Nicio acțiune nu va fi aplicată fişierelor ascunse. Aceste fişiere vor apărea în fişierul de raport.
Mută în carantină	Mută fişierele ascunse în carantină. Fişierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.
Demască	Demască fişierele ascunse astfel încât să le puteți vedea.

- **Opțiuni de acțiune pentru fișiere arhivate.** Scanarea și manevrarea fișierelor arhivate sunt supuse anumitor restricții. Arhivele protejate prin parolă nu pot fi scanate decât dacă furnizați parola. În funcție de formatul (tipul) arhivei, este posibil ca BitDefender să nu poată să dezinfecteze, să izoleze sau să șteargă fișierele arhivate infectate. Configurați acțiunile care vor fi aplicate asupra fișierelor arhivate detectate utilizând opțiunile adecvate din categoria **Opțiuni de acțiune pentru fișiere arhivate**.
  - Selectați acțiunea ce trebuie aplicată fișierelor infectate detectate. Următoarele opțiuni sunt disponibile:

Acțiune	*Descriere*
Nicio acțiune	Doar ține evidența fișierelor arhivate infectate 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.

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

Acțiune	*Descriere*
Nicio acțiune	Doar ține evidența fișierelor arhivate suspecte 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.

Acțiune	Descriere
Mută în carantină	Mută fişierele suspecte în carantină. Fişierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.

- Selectați acțiunea care trebuie aplicată fişierelor protejate prin parolă detectate. Următoarele opțiuni sunt disponibile:

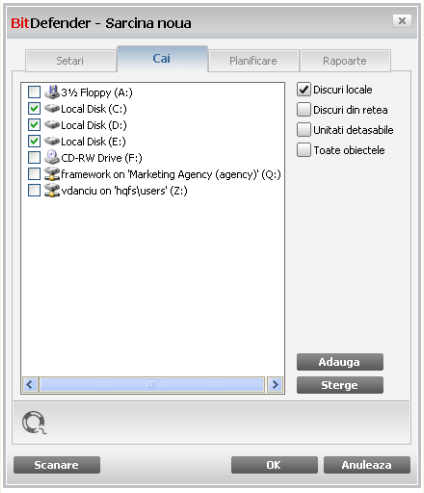
Acțiune	Descriere
Înregistrează ca nefiind scanate	Doar ține evidența fişierelor protejate prin parolă în raportul de scanare. După finalizarea scanării, puteți deschide raportul de scanare pentru a vedea informații despre aceste fişiere.
Cere parola	Atunci când este detectat un fişier protejat prin parolă, cere utilizatorului să furnizeze parola pentru a putea scana fişierul.

Notă
Dacă alegeți să ignorați fişierele detectate sau dacă acțiunea specificată eşuează, va trebui să alegeți o acțiune într-unul dintre paşii programului asistent de scanare.

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

Setarea locației de scanare

Pentru a seta locația de scanare a unei anumite sarcini de scanare, faceți clic-dreapta pe sarcină şi selectați **Schimbare cale**. Va apărea următoarea fereastră:



Locaţie scanare

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

Secțiunea conține următoarele butoane:

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

  Notă
  Puteți folosi drag & drop pentru a adăuga fişiere/directoare în listă.

- **Şterge obiect(e)** - şterge fişierele / directoarele care au fost selectate anterior din lista de obiecte de scanat.

  Notă
  Numai fişierele / directoarele adăugate de utilizator pot fi şterse, nu şi cele care au fost “văzute” automat de BitDefender.

Pe lângă butoanele explicate mai sus există şi unele opțiuni ce permit selectarea rapidă a locațiilor pentru scanare.

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

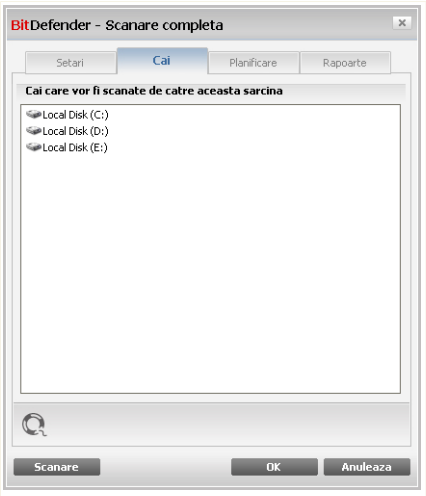
Notă
Dacă doriți să vă scanați tot sistemul, selectați opțiunea **Toate obiectele**.

Faceți clic pe **OK** pentru a salva modificările şi 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 vedea locația de scanare a unei anumite sarcini de scanare de sistem, faceți clic-dreapta pe sarcină şi selectați **Arată locații scanare**. Pentru sarcina **Scanare completă sistem**, de exemplu, va apărea următoarea fereastră:



Locații scanate de sarcina Scanare completă sistem

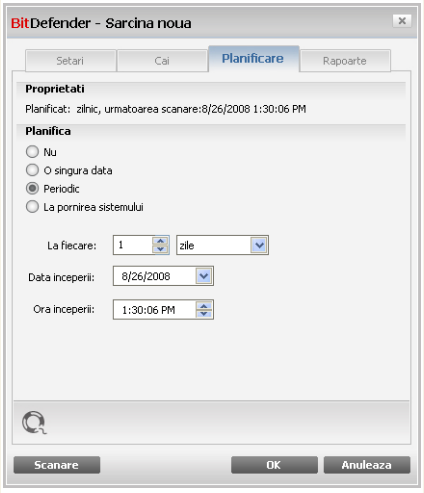
Sarcinile **Scanare completă sistem** şi **Scanare profundă sistem** scanează toate partițiile locale, în timp ce sarcina **Scanare rapidă sistem** scanează doar directoarele `Windows` şi `Program Files`.

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

Programarea sarcinilor de scanare

Pentru sarcini complexe procesul de scanare durează mai mult şi 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 vedea sau modifica programul de rulare a unei sarcini, faceți clic-dreapta pe sarcină şi selectați **Planificare sarcină**. Va apărea următoarea fereastră:



Programare scanări

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

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

- **Neplanificat** - sarcina este executată doar atunci când utilizatorul cere acest lucru.
- **O singură dată** - sarcina este executată o singură dată, la un anumit moment. Specificați data şi timpul lansării în execuție în câmpurile **Data începerii/Ora începerii**.
- **Periodic** - sarcina este executată periodic, la anumite intervale de timp(ore, zile, săptămâni, luni, ani), începând de la un anumit moment.

  Dacă doriți ca scanarea să se repete la anumite intervale de timp, selectați opțiunea **Periodic** şi introduceți în câmpul de editare **La fiecare** numărul de minute / ore / zile / săptămâni / luni / ani la care doriți să se repete scanarea. De asemenea, trebuie să specificați data şi timpul lansării în execuție în câmpurile **Data începerii/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 şi închide fereastra. Pentru a executa sarcina faceți clic pe **Scanează**.

15.2.5. Scanarea obiectelor

Înainte de a începe scanarea, este necesar să vă asigurați că BitDefender este la zi cu semnăturile de aplicații malițioase. Scanarea calculatorului folosind o bază de semnături veche 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 consola de setări.

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).

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 - când faceți clic-dreapta pe un fişier sau un director şi selectați opțiunea BitDefender Antivirus 2009.
- Scanare drag&drop - când aduceți un fişier sau director deasupra Barei de scanare.
- Scanare manuală - utilizați scanarea manuală BitDefender pentru a selecta direct fişierele şi 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.

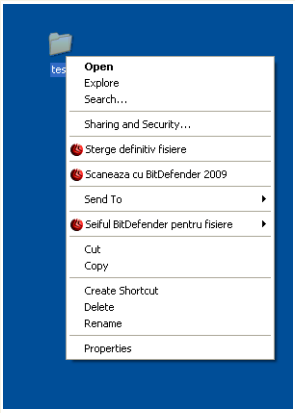
Pentru a rula o sarcină de scanare, utilizați una dintre următoarele metode:

- faceți dublu-clic pe sarcina de scanare dorită din listă.
- faceți clic pe butonul **Scanează acum** corespunzător sarcinii.
- selectați sarcina şi apoi faceți clic pe **Execută sarcina**.

Va apărea programul asistent de scanare şi scanarea va fi inițiată. Pentru mai multe informații, consultați “*Programul asistent de scanare*” (p. 204).

Scanare contextuală

Pentru a scana un fişier 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

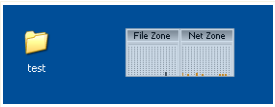
Faceți clic-dreapta pe fişierul sau directorul care doriți să fie scanat şi selectați opțiunea **BitDefender Antivirus 2009**.

Va apărea programul asistent de scanare şi scanarea va fi inițiată. Pentru mai multe informații, consultați "*Programul asistent de scanare*" (p. 204).

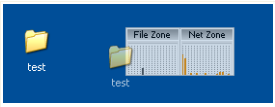
Puteți modifica opțiunile de scanare şi examina fişierele de raport accesând fereastra de **Proprietăți** a sarcinii **Scanare meniu contextual**.

Scanare prin drag&drop

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



Trageți fișierul



Lăsați fișierul

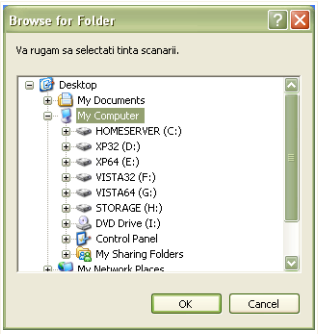
Va apărea programul asistent de scanare şi scanarea va fi inițiată. Pentru mai multe informații, consultați "*Programul asistent de scanare*" (p. 204).

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 şi 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 2009** → **Scanare manuală BitDefender**. Va apărea următoarea fereastră:



Scanare manuală

Selectați obiectul care doriți să fie scanat şi faceți clic pe **OK**.

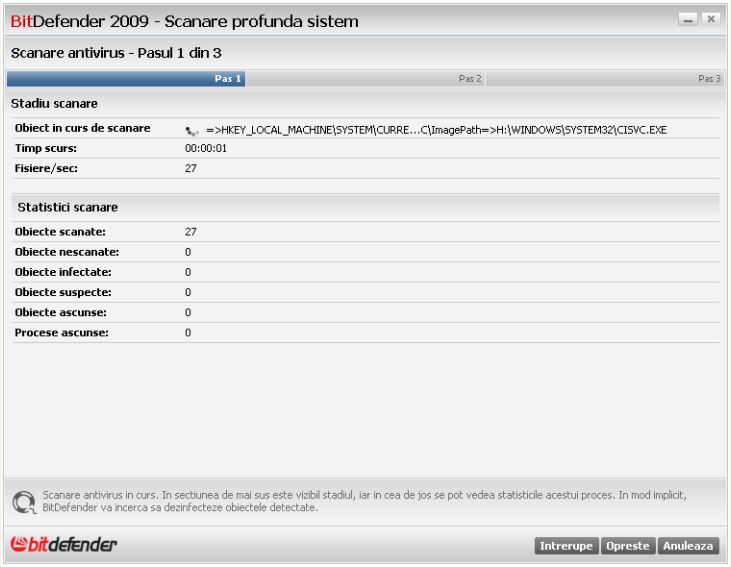
Va apărea programul asistent de scanare şi scanarea va fi inițiată. Pentru mai multe informații, consultați "*Programul asistent de scanare*" (p. 204).

Programul asistent de scanare

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

Pasul 1/3 - Scanare

BitDefender va începe scanarea obiectelor selectate.



Scanare

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

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

Pentru a opri temporar procesul de scanare, faceți clic pe **Întrerupe**. Va trebui să faceți clic pe **Reia** pentru a relua scanarea.

Puteți opri scanarea oricând doriți făcând clic pe **Stop&Da**. Veți sări direct la ultimul pas al programului asistent.

Aşteptați ca BitDefender să finalizeze 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 afişate 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.

Următoarele opțiuni pot apărea pe meniu:

Acțiune	Descriere
Nicio acțiune	Nu se va lua nicio acțiune asupra fişierelor detectate.
Dezinfectează	Dezinfectează fişierele infectate.
Şterge	Şterge fişierele detectate.
Demască	Face vizibile obiectele ascunse.

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 afişate într-o nouă fereastră.

Rezumat

Puteți vedea un rezumat al rezultatelor. Faceți clic pe **Afişează raport** pentru a vedea 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 fişierele infectate detectate sau va izola infecția. Cu toate acestea, există anumite probleme care nu pot fi rezolvate.

În aceste cazuri, vă recomandăm să contactaţi echipa de suport a BitDefender pe pagina web www.bitdefender.ro. Reprezentanţii noştri de suport tehnic vă vor ajuta să rezolvaţi problemele cu care vă confruntaţi.

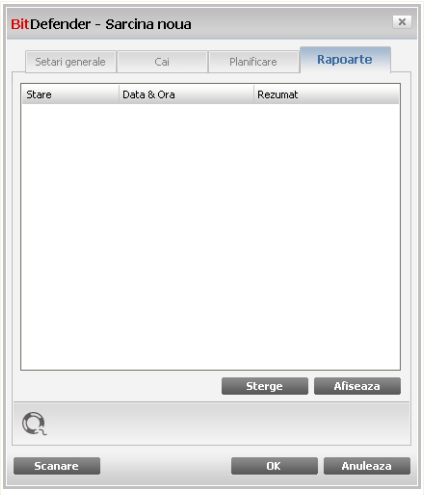
BitDefender a detectat fişiere suspecte

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

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

15.2.6. Examinarea rapoartelor de scanare

Pentru a examina rezultatele scanării după rularea unei sarcini, faceţi clic-dreapta pe sarcină şi selectaţi **Examinare rapoarte**. Va apărea următoarea fereastră:



Rapoarte

Aici puteţi examina rapoartele generate de fiecare dată când sarcina a fost executată. Pentru fiecare fişier sunt oferite informaţii privind situaţia procesului de scanare, data

şi timpul la care a fost executată scanarea precum şi un scurt rezumat al rezultatelor scanării.

Sunt disponibile două butoane:

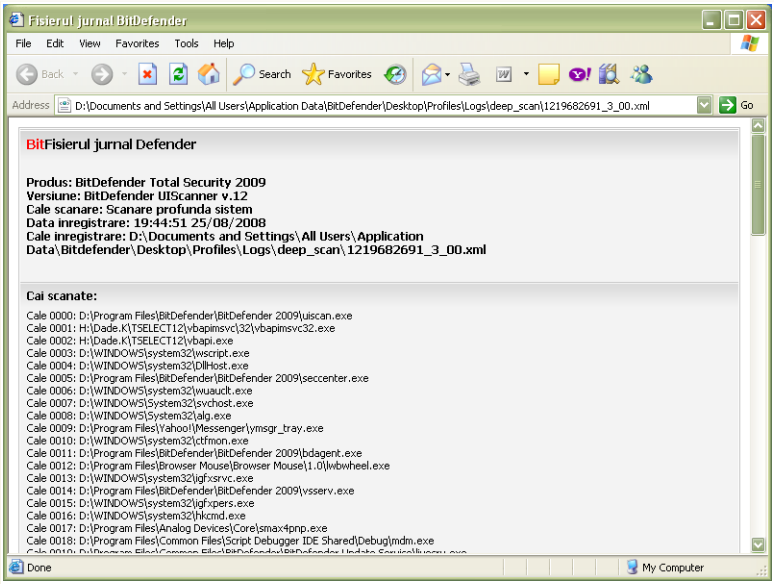
- **Şterge** - şterge fişierul de raport selectat.
- **Afişează** - deschide fişierul de raport selectat. Raportul de scanare va fi deschis în browserul dumneavoastră implicit.

Notă
De asemenea, pentru a deschide sau şterge un fişier de raport, faceți clic-dreapta pe fişier şi selectați opțiunea corespunzătoare din meniu.

Faceți clic pe **OK** pentru a salva modificările şi 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 şi acțiunile luate asupra acestor amenințări.

15.3. Obiecte excluse de la scanare

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

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

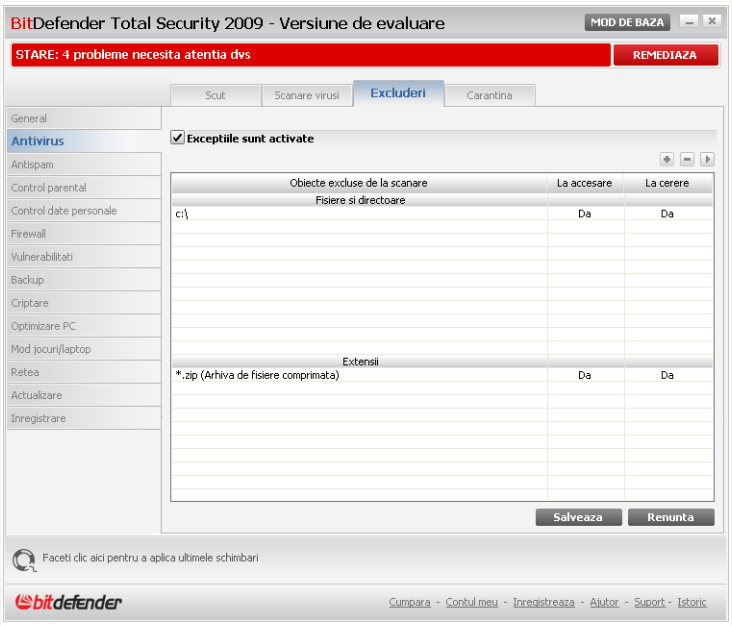
Pot fi excluse de la scanare două tipuri de obiecte:

- **Căi** - fişierul sau directorul (incluzând toate obiectele conținute) indicat de o cale specificată va fi exclus de la scanare.
- **Extensii** - toate fişierele 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 şi gestiona obiectele excluse de la scanare, mergeți la **Antivirus>Excepții** în modul avansat.



Excepții

Puteți vedea obiectele (fişiere, 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.

Pentru a şterge un obiect din listă, selectați-l şi faceți clic pe butonul **Şterge**.

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

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

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

15.3.1. 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.

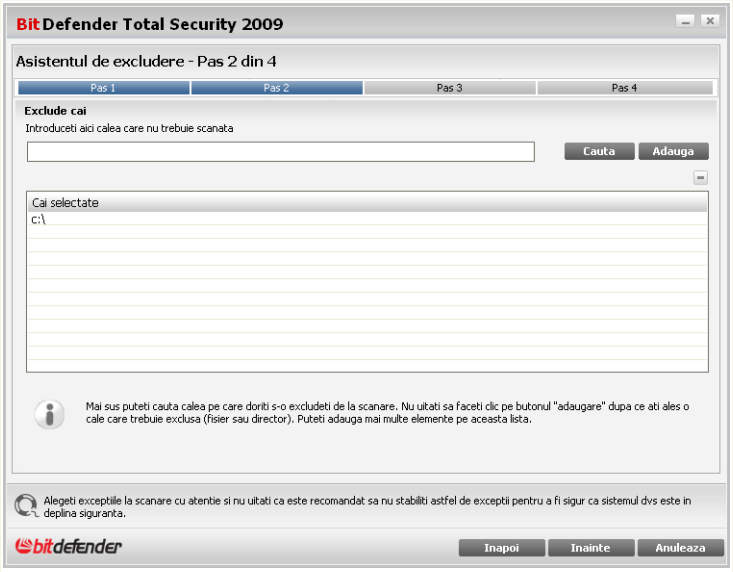
Pasul 1/4 - Selectați tipul obiectului

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

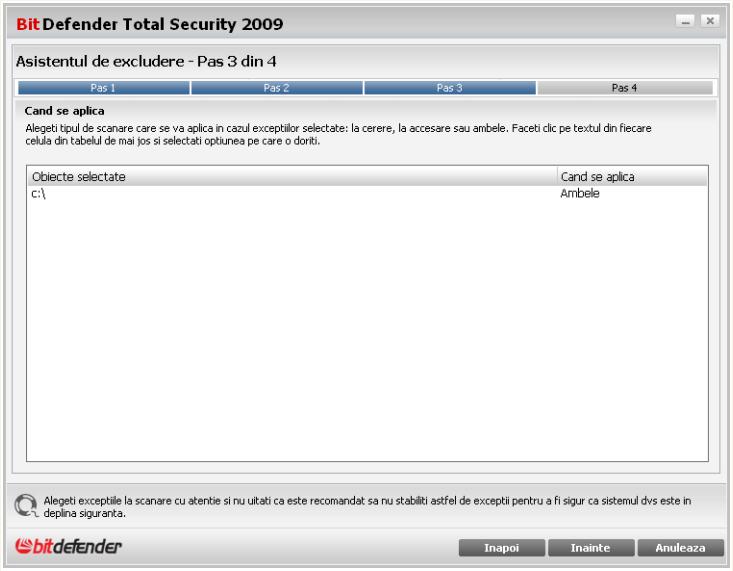
Notă
Un mesaj de eroare va apărea dacă nu există calea furnizată. Faceți clic pe **OK** şi verificați validitatea căii.

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

Pentru a şterge un obiect din listă, selectați-l şi faceți clic pe butonul **Şterge**.

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 şi tipul de scanare de la care acestea sunt excluse.

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

Faceți clic pe **Aplică** pentru a salva modificările.

15.3.2. 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.

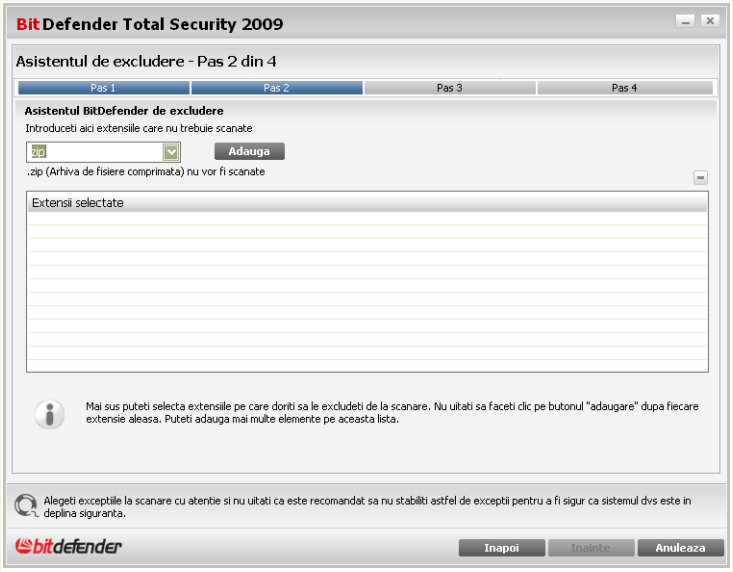
Pasul 1/4 - Selectați tipul obiectului

Tip obiect

Selectați opțiunea de excludere a unei extensii 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 şi 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.

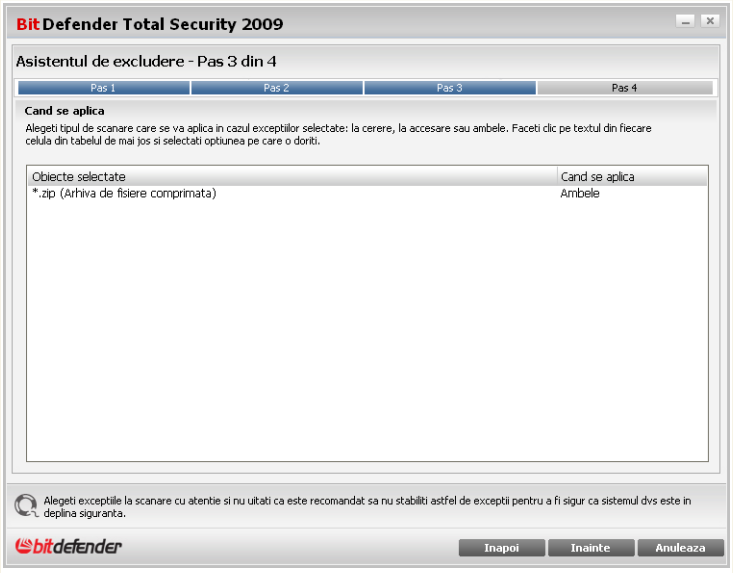
- Introduceți extensia care doriți să fie exclusă de la scanare şi faceți clic pe **Adaugă**.

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

Pentru a şterge un obiect din listă, selectați-l şi faceți clic pe butonul **Şterge**.

Faceți clic pe **Înainte**.

Pasul 3/4 - Selectați tipul de scanare



Tip scanare

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

Implicit, extensiile selectate sunt excluse atât de la scanarea la acces cât şi de la scanarea la cerere. Pentru a schimba când să fie aplicată excepția, faceți clic pe coloana din dreapta şi 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. Selectați căsuța pentru a scana aceste fișiere înainte de a le exclude de la scanare.

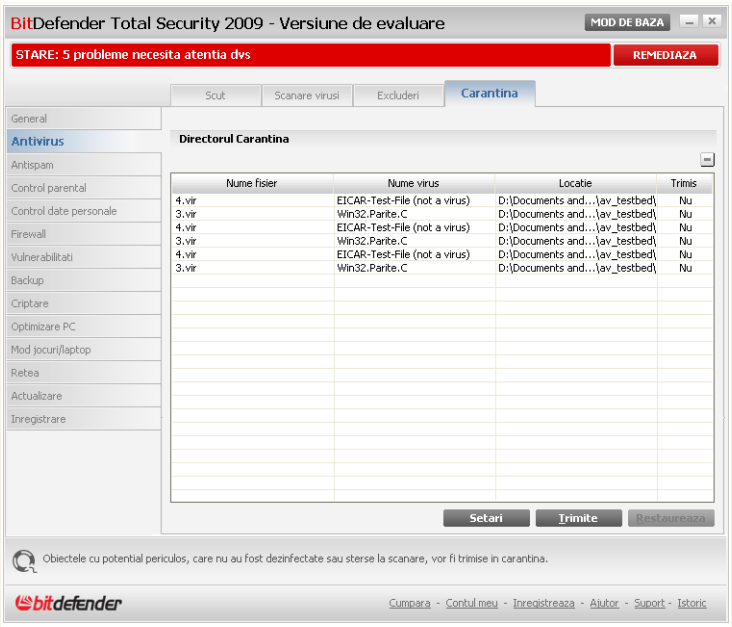
Faceți clic pe **Finalizare**.

Faceți clic pe **Aplică** pentru a salva modificările.

15.4. 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.

Pentru a vedea şi gestiona fişierele din carantină şi pentru a configura setările carantinei, mergeți la **Antivirus>Carantină** în modul avansat.



Carantină

Secțiunea Carantină afişează toate fişierele izolate în directorul Carantină. Puteți vedea numele fiecărui fişier, numele virusului detectat, calea către locația originală şi data trimiterii.

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

15.4.1. Gestionarea fişierelor din carantină

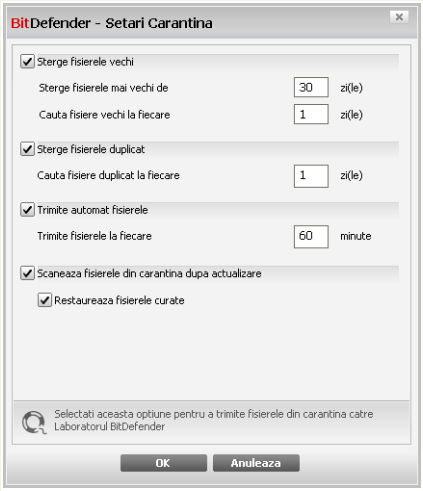
Pentru a şterge un fişier selectat din carantină faceți clic pe butonul **Şterge**. Dacă doriți să mutați fişierul selectat la locația originală faceți clic pe **Restaurează**.

Puteți trimite fișierele selectate la Laboratorul BitDefender pentru o analiză detaliată făcând clic pe **Trimite**.

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

15.4.2. 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:

Şterge fişierele vechi. Pentru a şterge automat fişierele vechi din carantină, bifați opțiunea corespunzătoare. Trebuie să specificați numărul de zile după care fişierele din carantină ar trebui şterse şi frecvența cu care BitDefender să caute fişiere vechi.

Notă
Implicit, BitDefender va căuta fişiere vechi în fiecare zi şi va şterge fişierele mai vechi de 10 zile.

Şterge fişierele duplicat. Pentru a şterge automat fişierele duplicat din carantină, bifați opțiunea corespunzătoare. Trebuie să specificați numărul de zile dintre două căutări consecutive de fişiere duplicat.

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

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

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

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

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

16. Antispam

BitDefender Antispam utlizează remarcabile inovații tehnologice şi filtre antispam standard pentru a ține la distanță spamul de căsuțele de mesaje ale utilizatorilor.

16.1. Detalii privind modulul Antispam

Spamul este o problemă în creştere, atât pentru individ cât şi 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) şi 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 şi mărimi.

16.1.1. Filtrele Antispam

Motorul BitDefender Antispam incorporează şapte 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) şi 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 cunoştințe sau chiar primesc mesaje de la companii sau organizații cu acelaşi domeniu de activitate. Folosind **listele de prieteni şi spammeri** îi puteți clasifica uşor 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 gestionate din modul avansat sau din bara de comenzi Antispam integrată în unii dintre cei mai folosiți clienți de mail.

Notă
Vă recomandăm să adăugați numele şi adresele prietenilor în **lista de prieteni**. BitDefender nu va bloca mesajele de la cei de pe listă; de aceea, adăugarea prietenilor în listă vă asigură că mesajele legitime vor ajunge în Inbox.

Filtrul de caractere

Multe mesaje Spam sunt scrise cu caractere chirilice şi / sau asiatice. Filtrul de caractere detectează acest tip de mesaje şi 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 ataşată. Pentru rezolvarea acestei probleme crescânde, BitDefender a introdus **Filtrul de imagini**, 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 şi oferă posibilitatea de a cumpăra obiecte şi, 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 şi 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 şi 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 şi 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, de exemplu, un anumit cuvânt format din patru litere apare mai des în mesajele Spam, atunci se poate presupune logic 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 şi stochează informații cu privire la toate mesajele. Pentru a funcționa eficient, filtrul trebuie educat, adică trebuie să i se dea exemple de Spam precum şi de mesaje legitime, la fel cum unui câine i se indică mirosul pe care trebuie să îl găsească. Uneori filtrul trebuie să fie şi corectat / atenționat atunci când clasifică greşit unele mesaje.

Important

Puteți corecta filtrul Bayesian folosind butoanele **Este Spam** şi **Nu este Spam** din bara de comenzi Antispam.

Notă

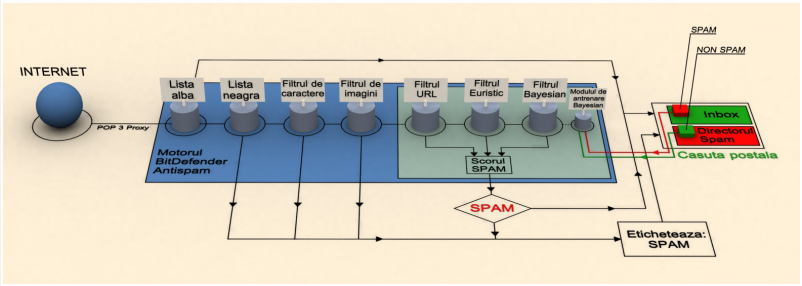
La fiecare actualizare:

- 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.

16.1.2. Funcționarea modulului Antispam

Schema de mai jos arată modul de funcționare al BitDefender Antispam.



Funcționarea modulului Antispam

Filtrele antispam din schema de mai sus (Lista de prieteni, Lista de spammeri, Filtrul de caractere, Filtrul de imagini, Filtrul URL, Filtrul NeuNet(euristic) şi Filtrul Bayesian) sunt folosite concomitent de către BitDefender, pentru a determina dacă un anume mesaj ar trebui sau nu să ajungă în **Inbox**.

Fiecare mesaj e-mail pe care îl primiți este întâi verificat de filtrul Lista de prieteni/Lista de spammeri. Dacă adresa expeditorului se regăseşte 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 regăseşte pe lista neagră, mesajul este etichetat ca SPAM şi 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 şi 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 ataşate imagini cu conținut spam.

Filtrul URL va căuta linkuri şi va compara linkurile găsite cu linkurile 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 şi va verifica toate componentele acestuia, căutând cuvinte, fraze, linkuri sau alte caracteristici spam. Şi 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 Bayesian va 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.

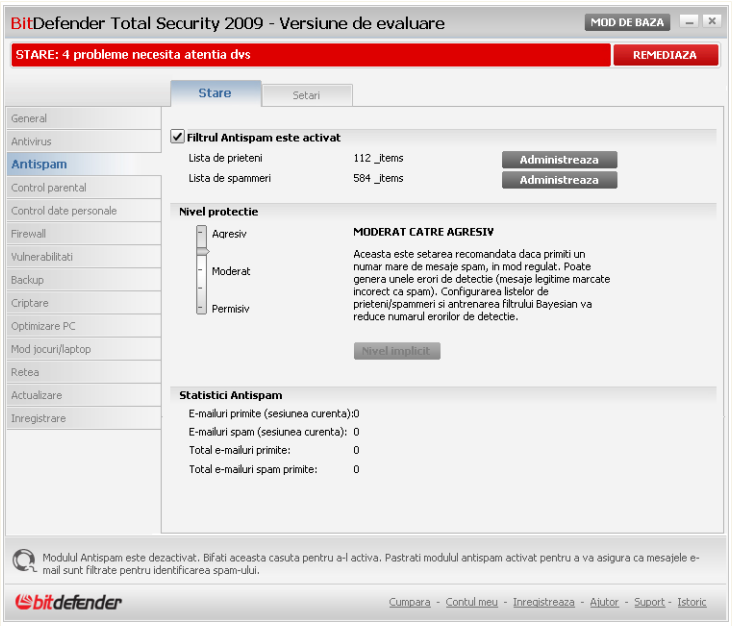
Dacă scorul Spam însumat (scorul URL + scorul Euristic + scorul Bayesian) depăşeşte scorul Spam pentru un mesaj (setat de către utilizator în secțiunea Antispam ca nivel de toleranță), mesajul este considerat SPAM.

Important

Dacă folosiți alt client de e-mail decât Microsoft Outlook sau Microsoft Outlook Express trebuie să creați o regulă prin care mesajele etichetate Spam de BitDefender să fie mutate într-un director de carantină. BitDefender adaugă prefixul [SPAM] în subiectul mesajelor considerate SPAM.

16.2. Stare

Pentru a configura protecția Antispam, mergeți la **Antispam>Status** în modul avansat.



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 sesiunea curentă (de când ați pornit calculatorul) sau un sumar al acesteia (de la instalarea BitDefender).

16.2.1. 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 nivele 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 obişnuite. 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**.

16.2.2. 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 ca Spam, chiar dacă au conținut asemănător mesajelor Spam.

Notã
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 şterge intrări din **lista de prieteni**.

Dacă doriți să adăugați o adresă, selectați **E-mail**, scrieți adresa şi faceți clic pe butonul . Adresa va apărea în **lista de prieteni**.

Important
Sintaxă: nume@domeniu.com.

Dacă doriți să adăugați un domeniu, selectați opțiunea **Domeniul**, scrieți domeniul şi faceți clic pe butonul . Domeniul va apărea în **lista de prieteni** .

Important
Sintaxă:

- @domeniu.com, *domeniu.com şi domeniu.com - toate mesajele primite de la domeniu.com vor ajunge în directorul **Inbox** indiferent de conținut;
- *domeniu* - toate mesajele primite de la domeniu (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 şterge un obiect din listă, selectați-l şi faceți clic pe butonul **Şterge**. Dacă faceți clic pe butonul **Şterge listă** veți şterge toate intrările din listă, dar atenție: este imposibil să le recuperați.

Folosiți butoanele **Salvare**/ **Încărcare** pentru a salva/încărca **lista de prieteni** într-o anume locație. Fişierul va avea extensia `.bwl`.

Pentru a reseta conținutul listei curente atunci când încărcați o listă salvată anterior selectați **Goleşte lista la încărcare**.

Notă
Vă recomandăm să adăugați numele şi adresele prietenilor în **lista de prieteni**. BitDefender nu va bloca mesajele de la cei de pe listă; de aceea, adăugarea prietenilor în listă vă asigură că mesajele legitime vor ajunge în Inbox.

Faceți clic pe **Salvare** şi **OK** pentru a salva modificările şi a închide **lista de prieteni**.

16.2.3. 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 şterge intrări din **lista de spammeri** .

Dacă doriți să adăugați o adresă, selectați **E-mail**, scrieți adresa şi faceți clic pe butonul . Adresa va apărea în **lista de spammeri**.

Important
Sintaxă: nume@domeniu.com.

Dacă doriți să adăugați un domeniu, selectați **Domeniul**, scrieți domeniul şi faceți clic pe butonul . Domeniul va apărea în **lista de spammeri**.

Important
Sintaxă:

- @domeniu.com, *domeniu.com and domeniu.com - toate mesajele primite de la domeniu.com vor fi etichetate ca SPAM;
- *domeniu* - toate mesajele primite de la domeniu(indiferent de sufixul domeniului) vor fi etichetate ca SPAM;
- *com - a- toate mesajele primite având sufixul domeniului com vor fi etichetate ca SPAM.

Pentru a şterge un obiect din listă, selectaţi-l şi faceţi clic pe butonul **Şterge**. Dacă faceţi clic pe butonul **Şterge listă** veţi şterge toate intrările din listă, dar atenţie: este imposibil să le recuperaţi.

Folosiţi butoanele **Salvare**/ **Încărcare** pentru a salva/încărca **lista de spammeri** într-o anumită locaţie. Fişierul va avea extensia `.bwl`.

Pentru a reseta conţinutul listei curente atunci când încărcaţi o listă salvată anterior selectaţi **Goleşte lista la încărcare**.

Faceţi clic pe **Salvare** şi **OK** pentru a salva modificările şi a închide **lista de spammeri**.

Important
Dacă doriţi să reinstalaţi BitDefender este recomandat să salvaţi listele de **Prieteni** / **Spammeri** înainte, iar după instalare le puteţi încărca.

16.3. Setări

Pentru a configura setările şi filtrele antispam, mergeţi la **Antispam>Setări** în modul avansat.

Setări Antispam

Sunt disponibile trei categorii de opțiuni (**Setări Antispam**, **Filtre Antispam elementare** şi **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.

16.3.1. 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.

16.3.2. Filtre Antispam elementare

- **Lista de prieteni/spammeri** - filtrează mesajele e-mail utilizând listele de prieteni /spammeri.
  - **Adaugă automat destinatarii la lista de prieteni** - adăugă automat destinatarii mesajelor trimise la lista de prieteni.
  - **Adaugă automat la lista de prieteni** - atunci când faceți clic pe butonul **Nu este spam** din bara de comenzi Antispam expeditorul este adăugat automat la lista de prieteni.
  - **Adaugă automat la lista de spammeri** - atunci când faceți clic pe butonul **Este Spam** din bara de comenzi Antispam expeditorul este adăugat automat la lista de spammeri.

Notă
Butoanele **Nu este Spam** şi **Este Spam** sunt folosite pentru educarea filtrului Bayesian.

- **Blochează mesaje scrise cu caractere asiatice** - blochează mesajele scrise cu caractere asiatice.
- **Blochează mesaje scrise cu caractere chirilice** - blochează mesajele scrise cu caractere chirilice.

16.3.3. 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.

17. Control parental

Controlul parental BitDefender vă permite să controlați accesul la Internet şi 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 şi mesajele instant care conțin anumite cuvinte cheie.
- jocuri, aplicații de chat, partajare de fişiere şi altele.
- mesaje instant trimise de alte contacte IM decât cele permise.

Important

Doar utilizatorii cu drepturi administrative pe sistem (administratorii de sistem) pot accesa şi 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 şi pe calculator ale copiilor dumneavoastră, trebuie să îndepliniți aceste sarcini principale:

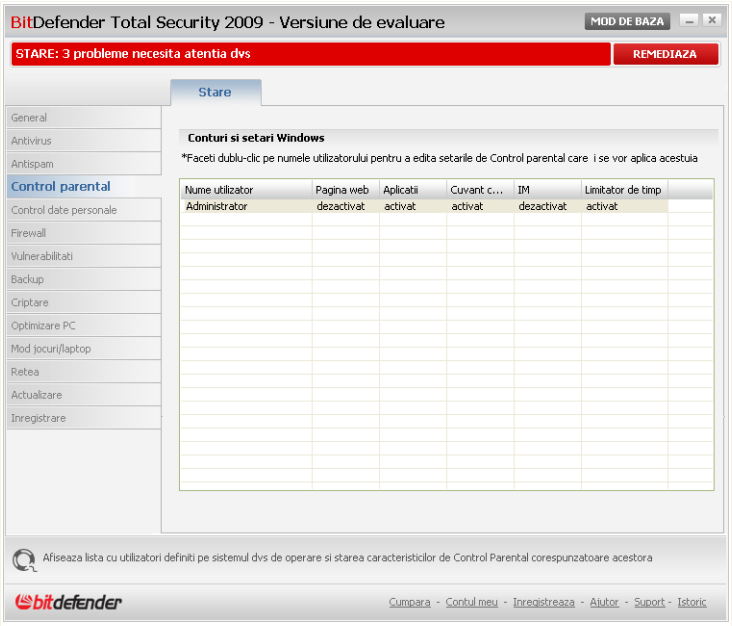
1. Creați conturi de utilizator Windows limitate (standard) pentru copiii dumneavoastră.

Notă

Pentru a afla cum să creați conturi de utilizator Windows, consultați Centrul de suport şi 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 avansat.



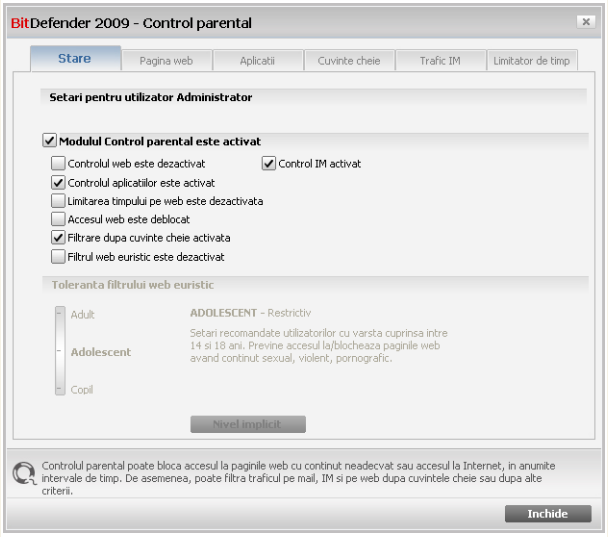
Control parental

Puteți vedea starea caracteristicilor de Control parental configurate pentru fiecare cont de utilizator Windows în parte. Faceți dublu-clic pe un nume de utilizator pentru a deschide fereastra în care puteți configura Controlul parental pentru respectivul cont de utilizator.

Următoarele secțiuni din acest capitol prezintă în detaliu caracteristicile de Control parental şi cum să le configurați.

17.1. Starea setărilor pentru un utilizator

Pentru a configura Controlul parental pentru un anumit utilizator, faceți dublu-clic pe utilizatorul respectiv şi faceți clic pe tabul **Status**.



Status Control parental

Pentru a configura Controlul parental pentru acest cont de utilizator, urmați aceşti paşi:

1. Activați Controlul parental pentru acest cont de utilizator selectând căsuța corespunzătoare opțiunii **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. 240).
3. Selectați căsuțele corespunzătoare controalelor de protecție pe care doriți să le utilizați:
   - **Control Web** - pentru a filtra navigarea în rețea conform regulilor stabilite de dumneavoastră în secțiunea Web.

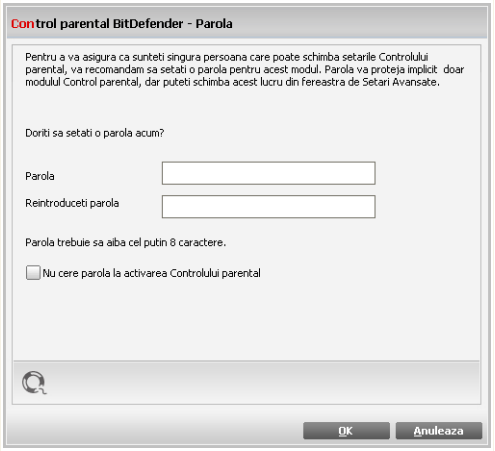
- **Control aplicații** - pentru a bloca accesul la aplicații de pe calculator conform regulilor stabilite de dumneavoastră în secțiunea Aplicații.
- **Control mesagerie instant** - pentru a bloca sau permite conversațiile cu utilizatori de mesagerie instant conform regulilor stabilite de dumneavoastră în secțiunea Trafic IM.
- **Limitator de timp** - pentru a permite accesul la rețea conform orarului stabilit de dumneavoastră în secțiunea Timp.
- **Acces web** - pentru a bloca accesul la toate paginile web (nu doar la cele din secțiunea Web).
- **Filtrare cuvinte** - pentru a filtra accesul la web, mail şi mesageria instant conform regulilor stabilite de dumneavoastră în secțiunea Cuvinte.
- **Filtru web euristic** - pentru a filtra accesul web conform unor reguli prestabilite bazate pe categorii de vârstă.

4. Pentru a beneficia de caracteristicile oferite de Controlul Parental, trebuie să configurați controalele selectate. Pentru a afla cum să le configurați, consultați următoarele secțiuni din acest capitol.

17.1.1. 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 şi 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 şi nu doriți să mai apară această fereastră din nou, bifați **Nu solicita parolă la activarea Controlului parental**.

17.1.2. Configurarea filtrului web euristic

Filtrul web euristic analizează paginile web şi 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 nivele de toleranță:

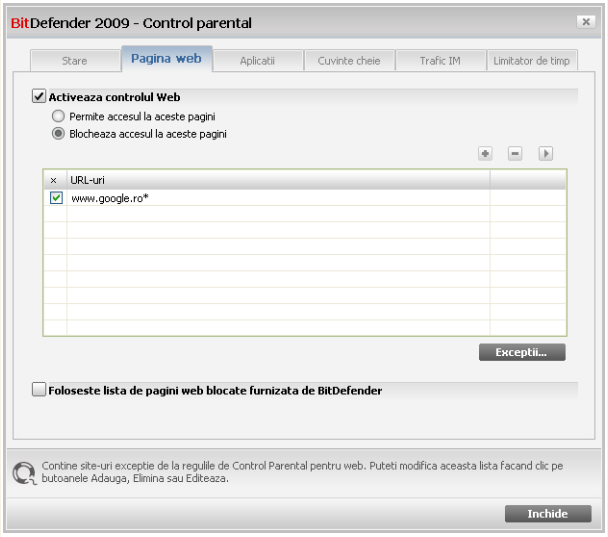
Nivelul de toleranță	*Descriere*
Copil	Oferă acces web restricționat, conform setărilor recomandate pentru utilizatori mai mici de 14 ani. Paginile web cu conținut potențial dăunător pentru copii (pornografie, sexualitate, droguri, hacking etc.) sunt blocate.
Adolescent	Oferă acces web restricționat, conform setărilor recomandate pentru utilizatori având vârsta între 14 şi 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.

17.2. 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 şi actualizată permanent, ca parte a procesului obişnuit de actualizare.

Pentru a configura Controlul web pentru un anumit utilizator, faceți dublu-clic pe utilizatorul respectiv şi faceți clic pe tabul **Web**.



Control Web

Pentru a activa această protecție selectați căsuța corespunzătoare opțiunii **Activează controlul web**.

Selectați **Permite accesul la aceste pagini**/**Blochează accesul la aceste pagini** pentru a vedea lista paginilor permise/blocate. Faceți clic pe **Excepții...** pentru a accesa lista complementară.

Regulile trebuie introduse manual. Mai întâi, selectați **Permite accesul la aceste pagini**/**Blochează accesul la aceste pagini** pentru a permite/bloca accesul la paginile pe care le veți specifica în cadrul asistentului. Apoi, faceți clic pe butonul **Adaugă...** pentru a deschide asistentul de configurare.

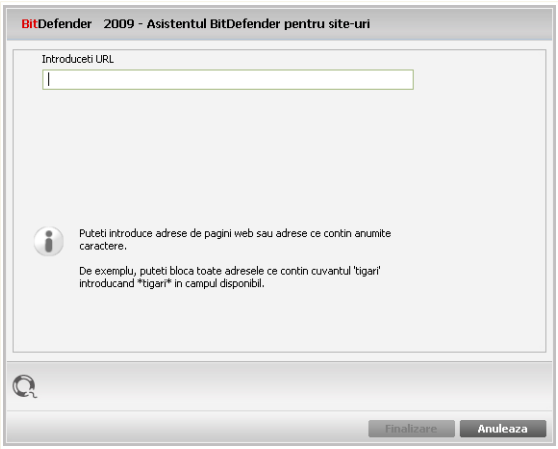
Pentru a şterge o regulă, selectați-o şi faceți clic pe butonul **Şterge**. Pentru a modifica o regulă, selectați-o şi faceți clic pe butonul **Editează** sau faceți dublu-clic pe ea. Pentru a dezactiva temporar o regulă fără a o şterge, deselectați căsuța corespunzătoare.

Faceți clic pe **Aplică** pentru a salva modificările.

17.2.1. Asistentul de configurare

Asistentul de configurare este o procedură constituită dintr-un singur pas.

Pasul 1/1 - Specificați paginile



Specificați paginile

Introduceți pagina pentru care se va aplica regula şi faceți clic pe **Finalizare**.

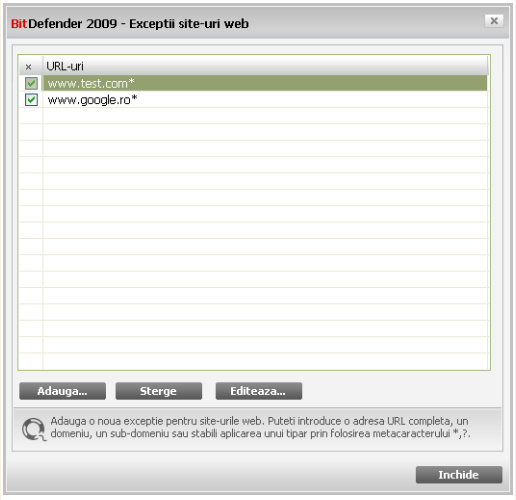
Important
Sintaxă:

- `*.xxx.com` - acțiunea regulei se va aplica asupra tuturor paginilor terminate în `.xxx.com`;
- `*porn*` - acțiunea regulei se va aplica asupra tuturor paginilor ce conțin cuvântul `porn` în adresă;
- `www.*.com` - acțiunea regulei se va aplica asupra tuturor paginilor având sufixul domeniului `com`;
- `www.xxx.*` - acțiunea regulei se va aplica asupra tuturor paginilor ce încep cu `www.xxx.` indiferent de sufixul domeniului.

17.2.2. Specificați excepțiile

Uneori poate fi nevoie să specificați excepții de la o anumită regulă. De exemplu, stabiliți o regulă care blochează paginile ce conțin cuvântul "killer" în adresă (sintaxă: `*killer*`). De asemenea, cunoaşteți un site numit `killer-music` unde vizitatorii pot asculta muzică online. Pentru a crea o excepție la regula stabilită anterior, accesați fereastra **Excepții** şi definiți o excepție de la regulă.

Faceți clic pe **Excepții...**. Va apărea următoarea fereastră:



Specificare excepții

Faceți clic pe **Adaugă...** pentru a specifica excepțiile. Va apărea asistentul de configurare. Finalizați asistentul pentru a stabili excepția.

Pentru a şterge o regulă, selectați-o şi faceți clic pe butonul **Şterge**. Pentru a modifica o regulă, selectați-o şi faceți clic pe butonul **Editează** sau faceți dublu-clic pe ea. Pentru a dezactiva temporar o regulă fără a o şterge, deselectați căsuța corespunzătoare.

Faceți clic pe **Închide** pentru a salva modificările şi închide fereastra.

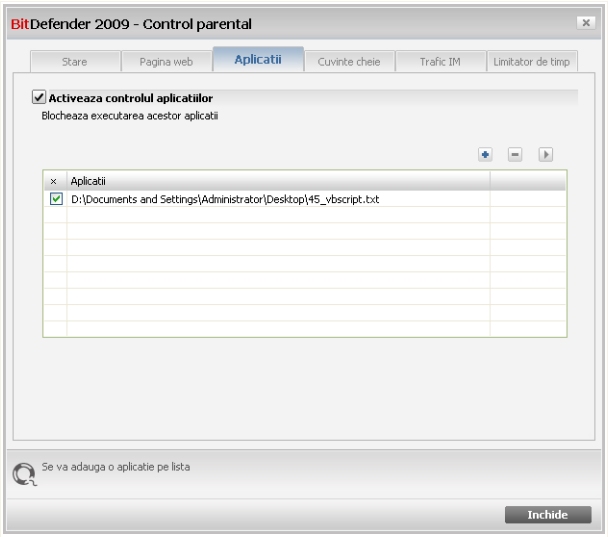
17.2.3. Lista web neagră a BitDefender

Pentru a vă ajuta să vă protejați copiii, BitDefender furnizează o listă neagră de pagini web având conținut inadecvat sau potențial periculos. Pentru a bloca paginile ce apar pe această listă selectați **Foloseşte lista de site-uri blocate furnizată de BitDefender**.

17.3. Control aplicații

Controlul aplicațiilor vă ajută să împiedicați orice aplicație să ruleze. Jocurile, softul media şi de mesagerie, precum şi alte categorii de soft şi aplicații malițioase pot fi împiedicate să ruleze. Aplicațiile blocate în acest fel sunt de asemenea protejate de modificări, şi nu pot fi copiate sau mutate.

Pentru a configura Controlul aplicațiilor pentru un anumit utilizator, faceți dublu-clic pe utilizatorul respectiv şi faceți clic pe tabul **Aplicații**.



Control aplicații

Pentru a activa această protecție selectați căsuța corespunzătoare opțiunii **Activează controlul aplicațiilor**.

Regulile trebuie introduse manual. Faceți clic pe butonul **Adaugă** pentru a deschide asistentul.

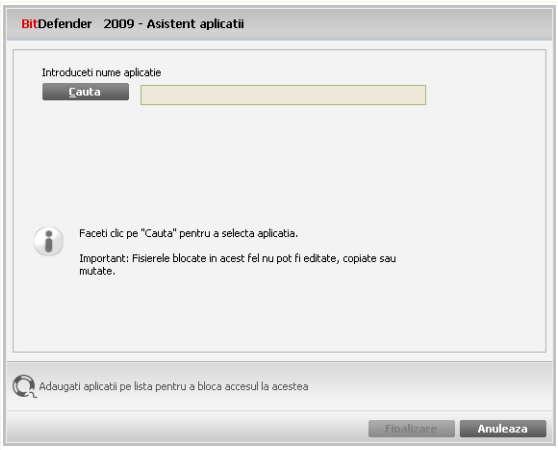
Pentru a şterge o regulă, selectați-o şi faceți clic pe butonul **Şterge**. Pentru a modifica o regulă, selectați-o şi faceți clic pe butonul **Editează** sau faceți dublu-clic pe ea. Pentru a dezactiva temporar o regulă fără a o şterge, deselectați căsuța corespunzătoare.

Faceți clic pe **Aplică** pentru a salva modificările.

17.3.1. Asistentul de configurare

Asistentul de configurare este o procedură constituită dintr-un singur pas.

Pasul 1/1 - Selectați aplicația ce va fi blocată



Selectați aplicația ce va fi blocată

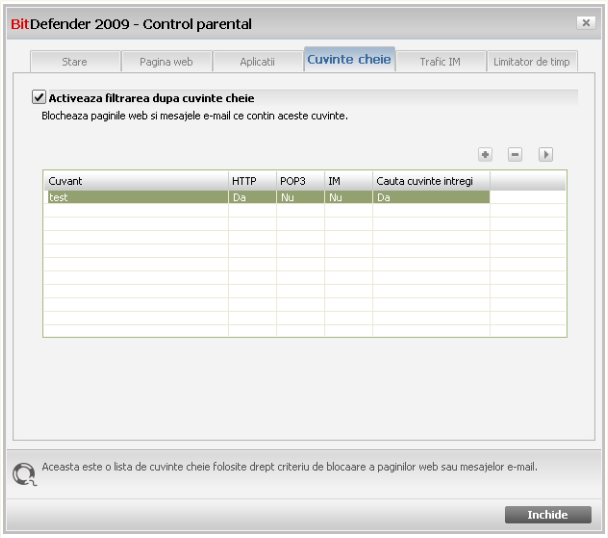
Faceți clic pe **Caută**, selectați aplicația care doriți să fie blocată şi faceți clic pe **Finalizare**.

17.4. Filtrare cuvinte

Filtrarea după cuvinte vă ajută să blocați accesul utilizatorilor la mesaje e-mail, pagini web şi mesaje instant care conțin anumite cuvinte. Utilizând Filtrarea după cuvinte, puteți preveni vizualizarea de cuvinte sau expresii nepotrivite de către copiii dumneavoastră, atunci când aceştia sunt online.

Notă
Filtrarea după cuvinte a mesageriei instant este disponibilă doar pentru Yahoo Messenger şi Windows Live (MSN) Messenger.

Pentru a configura Filtrarea după cuvinte pentru un anumit utilizator, faceți dublu-clic pe utilizatorul respectiv şi faceți clic pe tabul **Cuvinte**.



Filtrare cuvinte

Selectați căsuța **Activează filtrarea după cuvinte** pentru a utiliza această caracteristică.

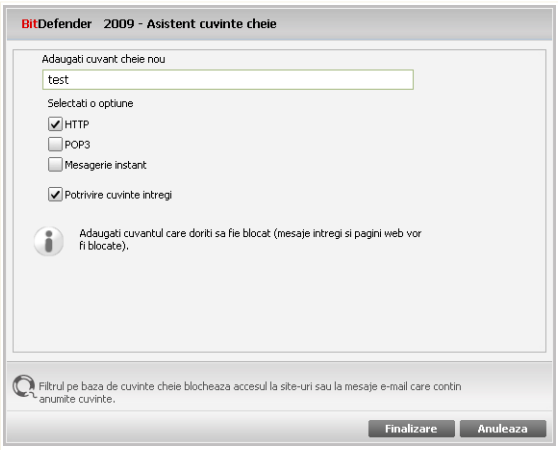
Trebuie să adăugați reguli pentru a preciza cuvintele cheie care să fie blocate. Pentru a adăuga o regulă, faceți clic pe butonul **Adaugă** şi configurați parametrii regulii în fereastra de configurare.

Pentru a şterge o regulă, selectați-o şi faceți clic pe butonul **Şterge**. Pentru a edita o regulă, faceți dublu-clic pe aceasta sau faceți clic pe butonul **Editează** şi efectuați modificările dorite în fereastra de configurare.

Faceți clic pe **Aplică** pentru a salva modificările.

17.4.1. Fereastra de configurare

Atunci când adăugați sau editați reguli, va apărea fereastra de configurare.



Introduceți cuvântul cheie

Trebuie setați parametrii următori:

- **Cuvânt cheie** - introduceți în câmpul editabil cuvântul sau fraza pe care vreți să o blocați.
- **Protocol** - alegeți protocolul pe care BitDefender să-l scaneze în căutarea argumentului specificat.

Opțiune	Descriere
POP3	Mesajele e-mail care conțin argumentul sunt blocate.
HTTP	Paginile web care conțin argumentul sunt blocate.
Mesagerie instant	Mesajele instant care conțin argumentul sunt blocate.

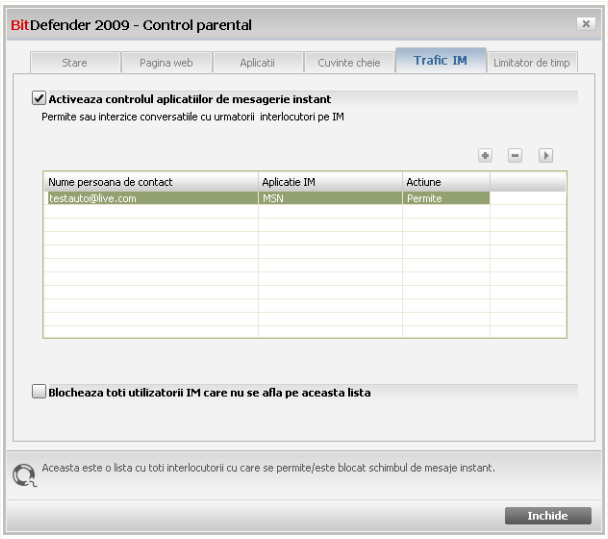
Faceți clic pe **Finalizare** pentru a adăuga regula.

17.5. 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 şi Windows Live (MSN) Messenger.

Pentru a configura Controlul IM pentru un anumit utilizator, faceți dublu-clic pe utilizatorul respectiv şi faceți clic pe tabul **Trafic IM**.



Controlul mesageriei instant

Selectați căsuța **Activează Controlul mesageriei instant** dacă doriți să utilizați această caracteristică de control.

Trebuie să adăugați reguli pentru a preciza contactele cu care utilizatorul are sau nu voie să converseze. Pentru a adăuga o regulă, faceți clic pe butonul **Adaugă** şi configurați parametrii regulii în fereastra de configurare.

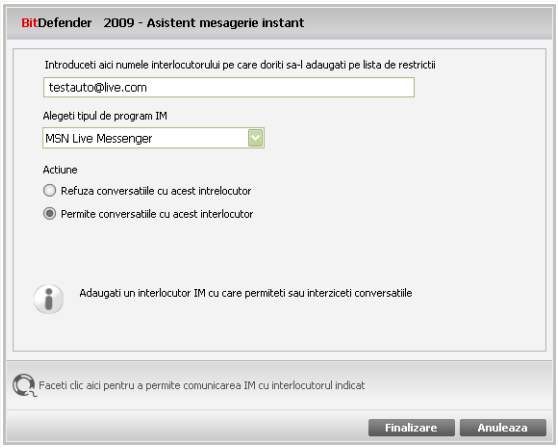
Pentru a şterge o regulă, selectați-o şi faceți clic pe butonul **Şterge**. Pentru a edita o regulă, faceți dublu-clic pe aceasta sau faceți clic pe butonul **Editează** şi efectuați modificările dorite în fereastra de configurare.

Dacă ați definit toate contactele de mesagerie instant cu care utilizatorul are voie să converseze, selectați **Blochează toți utilizatorii IM care nu sunt în această listă**. Astfel, doar contactele de mesagerie instant permise în mod explicit vor putea trimite mesaje instant utilizatorului.

Faceți clic pe **Aplică** pentru a salva modificările.

17.5.1. Fereastra de configurare

Atunci când adăugați sau editați reguli, va apărea fereastra de configurare.



Adăugați contacte IM

Procedați astfel:

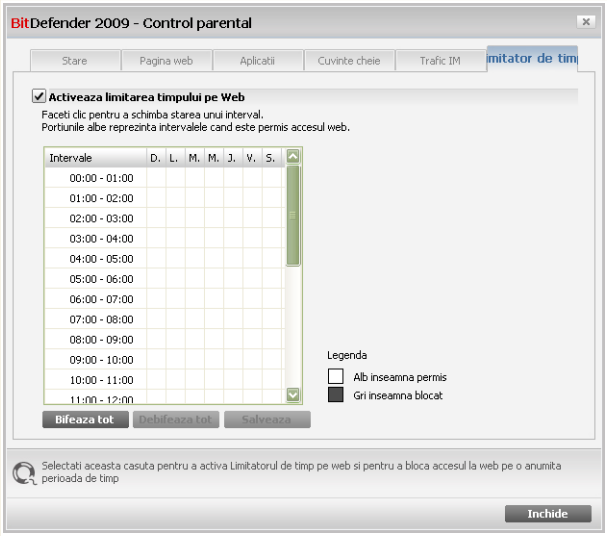
1. Introduceți numele de utilizator (ID-ul) contactului de mesagerie instant.
2. Selectați programul de mesagerie instant asociat contactului.
3. Selectați acțiunea regulii:
   - **Blochează conversațiile cu acest contact**
   - **Permite conversațiile cu acest contact**
4. Faceți clic pe **Finalizare** pentru a adăuga regula.

17.6. 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.

Notã
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 dublu-clic pe utilizatorul respectiv şi faceți clic pe tabul **Timp**.



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 internet vor fi blocate. Puteți face clic pe celule individuale, sau puteți face clic şi apoi să trageți cursorul de-a lungul celulelor pentru a acoperi intervale mai mari de timp. De asemenea, puteți face clic pe **Bifează tot** pentru a selecta toate căsuțele şi, implicit, a bloca accesul la rețea. Dacă faceți clic pe **Debifează tot**, conexiunile la Internet vor fi permise tot timpul.

Important
Căsuțele colorate în gri reprezintă intervalele de timp când toate conexiunile internet sunt blocate.

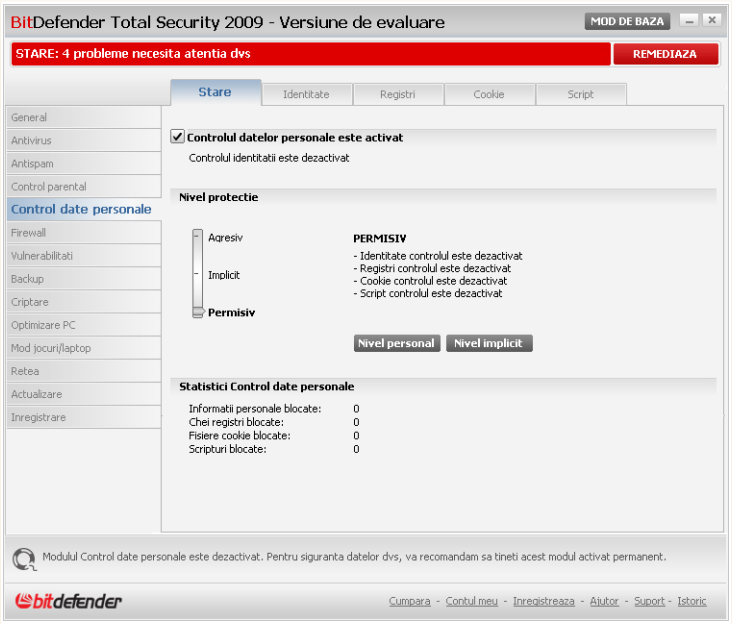
Faceți clic pe **Aplică** pentru a salva modificările.

18. Control date

BitDefender monitorizează zeci de potențiale puncte sensibile ale sistemului dumneavoastră de operare, acolo unde pot acționa aplicațiile spyware, şi verifică orice schimbare apărută. Acest modul blochează în mod eficient caii troieni şi alte instrumente instalate de hackeri, care încearcă să vă dezvăluie identitatea şi să trimită informațiile personale, cum ar fi seria cărții de credit,din computerul dumneavoastră, către hacker.

18.1. Status Control date

Pentru a configura Controlul datelor şi a vedea informații legate de activitatea sa, faceți clic pe **Control date>Status** în modul avansat.



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 şi 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) şi de mesagerie instant la ieşirea din calculator potrivit regulilor create de dumneavoastră în secțiunea Identitate.
- Controlul regiştrilor - vă cere permisiunea de fiecare dată când un program încearcă să modifice informațiile din regiştri astfel încât să fie lansat la pornirea Windows.
- Controlul fişierelor 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**.

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	Doar **Controlul regiştrilor** este activat.
Standard	**Controlul regiştrilor** şi **Controlul identității** sunt activate.
Agresiv	**Controlul regiştrilor**, **Controlul identității** şi **Controlul scripturilor** sunt activate.

Puteți personaliza nivelul de protecție făcând clic pe **Nivel personal**. În fereastra care va apărea, selectați controalele de protecție pe care doriți să le activați şi faceți clic pe **OK**.

Faceți clic pe **Nivel implicit** pentru a seta cursorul la nivelul implicit.

18.2. 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 şi se foloseşte 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, căutând anumite şiruri de caractere (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 şi folosi propriile reguli de protecție a identității. Regulile pe care le creați sunt aplicate şi pot fi accesate doar atunci când sunteți conectat în Windows de pe contul dumneavoastră de utilizator.

De ce să utilizați Controlul identității?

- Controlul identității este foarte eficient în blocarea aplicațiilor spyware keylogger. Acest tip de aplicații malițioase înregistrează tot ceea ce tastați şi trimite aceste înregistrări prin Internet către o persoană malițioasă (un hacker). Hackerul poate afla din datele furate informații confidențiale, cum ar fi parole şi numere de conturi bancare, pe care le va folosi în beneficiul propriu.

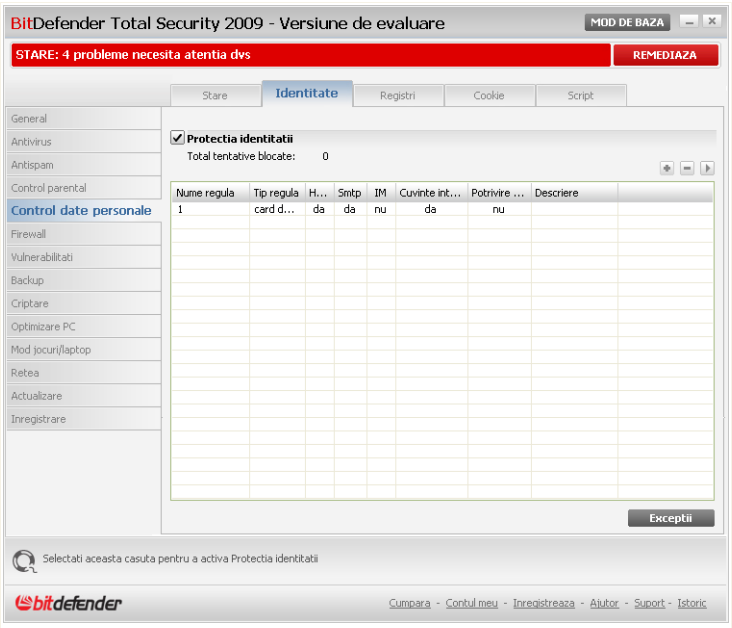
  În eventualitatea în care o astfel de aplicație reuşeşte să evite detecția antivirus, aceasta nu va putea trimite datele furate prin e-mail, web sau mesaje instant, dacă ați creat reguli adecvate de protecție a identității.

- 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 înşelător 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 şi 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. Deşi par a fi legitime, e-mailul şi pagina web spre care vă trimite linkul înşelător sunt false. Dacă faceți clic pe linkul din e-mail şi trimiteți informațiile dumneavoastră personale de pe pagina web falsă, veți dezvălui aceste informații persoanelor răuvoitoare care au organizat înşelătoria.

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>Identitate** în modul avansat.



Control identitate

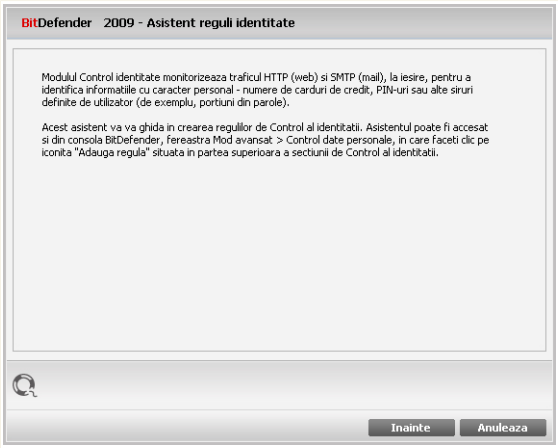
Dacă doriți să utilizați Controlul identității, urmați aceşti paşi:

1. Selectați căsuța **Control identitate**.
2. Creați reguli pentru a vă proteja datele confidențiale. Pentru mai multe informații, consultați "*Crearea regulilor de identitate*" (p. 259).
3. Daca este nevoie, definiți excepții specifice de la regulile pe care le-ați creat. Pentru mai multe informații, consultați "*Specificarea excepțiilor*" (p. 262).

18.2.1. Crearea regulilor de identitate

Pentru a crea o regulă de protecție a identității, faceți clic pe butonul **Adaugă** şi urmați paşii programului asistent.

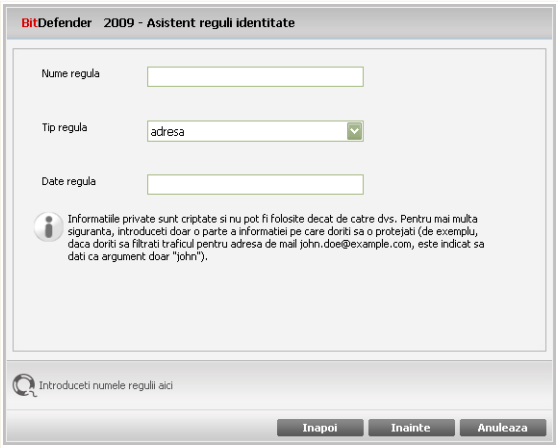
Pasul 1/4 - Fereastra de întâmpinare



Fereastra de întâmpinare

Faceți clic pe **Înainte**.

Pasul 2/4 - Furnizați tipul și argumentul regulei



Furnizați tipul și argumentul regulei

Trebuie setați parametrii următori:

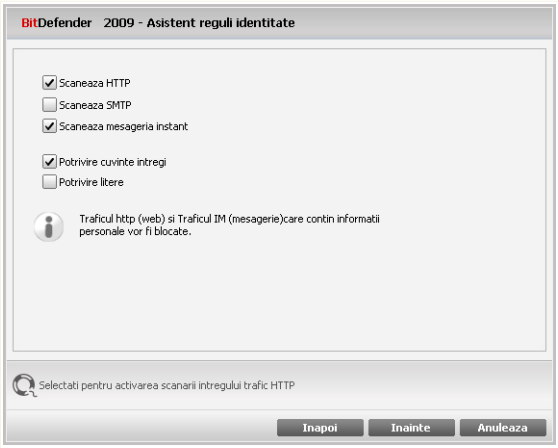
- **Nume regulă** - introduceți numele regulii în acest câmp editabil.
- **Tip regulă** - alegeți tipul regulei (adresă, nume, card de credit, PIN, etc.).
- **Date regulă** - introduceți datele pe care doriți să le protejați în acest câmp editabil. De exemplu, pentru a vă proteja numărul cardului dumneavoastră 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 traficul



Selectați traficul

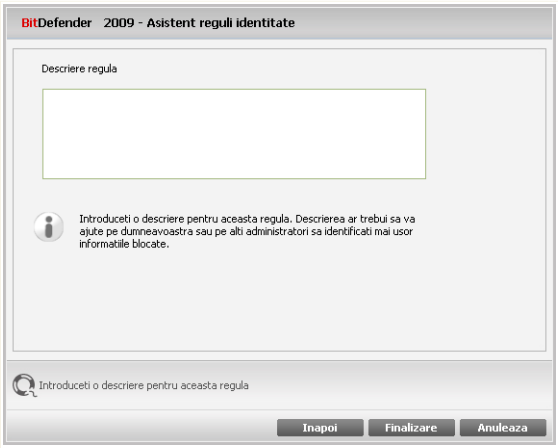
Selectați tipul de trafic care doriți să fie scanat de BitDefender. Următoarele opțiuni sunt disponibile:

- **Scanează HTTP** - scanează traficul HTTP (web) şi blochează la ieşire toate datele care corespund unei reguli.
- **Scanează SMTP** - scanează traficul SMTP (mail) şi blochează trimiterea mesajelor e-mail care corespund unei reguli.
- **Scanează mesageria instant** - scanează traficul de mesagerie instant şi blochează trimiterea mesajelor instant care corespund unei reguli.

Puteți alege să aplicați regula doar dacă datele protejate apar ca şir independent sau ținând cont de majuscule şi minuscule.

Faceți clic pe **Înainte**.

Pasul 4/4 - Descrieți regula



Descrieți regula

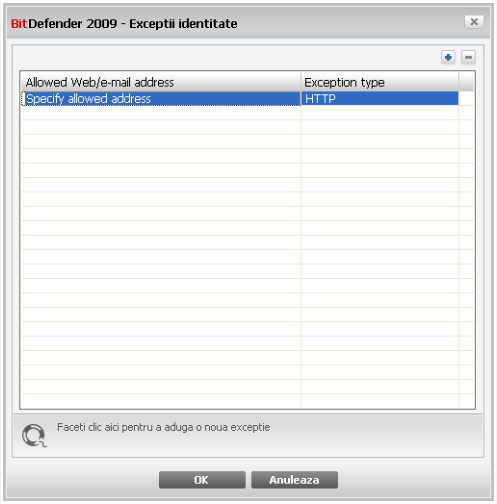
Introduceți o scurtă descriere a regulei în câmpul editabil. Deoarece informația blocată (şirul respectiv de caractere) nu este afişată atunci când este accesată regula, descrierea trebuie să ajute la identificarea acesteia.

Faceți clic pe **Finalizare**. Regula va apărea în tabel.

18.2.2. Specificarea excepțiilor

În unele cazuri, este nevoie să definiți excepții la 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 ştiți că este securizat), va trebui să specificați o excepție de la regula respectivă.

Pentru a deschide fereastra unde puteți gestiona excepțiile, faceți clic pe **Excepții**.



Excepții

Pentru a adăuga o excepție, urmați aceşti paşi:

1. Faceți clic pe **Adaugă** pentru a adăuga o nouă înregistrare în listă.
2. Faceți dublu-clic pe **Specificați adresa permisă** şi introduceți site-ul web, adresa de e-mail sau contactul IM care doriți să fie adăugate ca excepție.
3. Faceți dublu-clic pe **Alegeți tipul** şi alegeți din meniu opțiunea corespunzătoare tipului de adresă furnizată anterior.
   - Dacă ați specificat o adresă web, selectați **HTTP**.
   - Dacă ați specificat o adresă de mail, selectați **SMTP**.
   - Dacă ați specificat un contact IM, selectați **IM**.

Pentru a şterge o excepție din listă, selectați-o şi faceți clic pe **Şterge**.

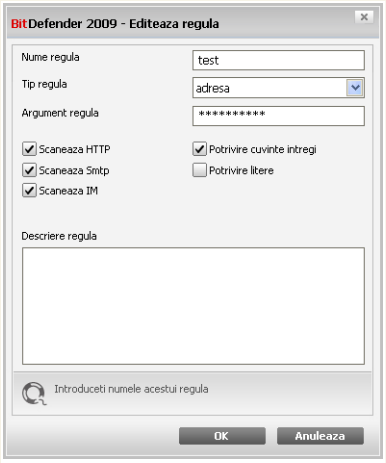
Faceți clic pe **OK** pentru a salva modificările.

18.2.3. Administrarea regulilor

Puteți vedea listate în tabel regulile create până în momentul de față.

Pentru a şterge o regulă, selectați-o şi faceți clic pe butonul **Şterge**.

Pentru a modifica atributele unei reguli, selectați-o şi faceți clic pe butonul **Editează** sau faceți dublu-clic pe ea. Va apărea o nouă fereastră.



Editează regula

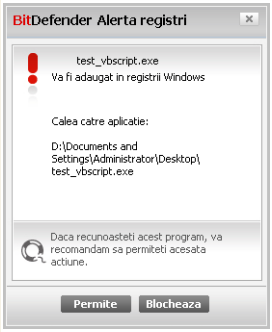
Aici puteți modifica numele, descrierea şi parametrii regulei (tip, argument şi trafic). Faceți clic pe **OK** pentru a salva modificările.

18.3. Control regiştri

Una dintre părțile importante ale sistemului de operare Windows sunt **regiştrii**. Aici îşi păstrează Windows configurația şi setările, programele instalate, informații despre utilizator şi alte date.

Tot în **regiştri** sunt definite programele care sunt lansate la pornirea Windows. Viruşii folosesc des această caracteristică Windows pentru a se lansa automat atunci când utilizatorul îşi reporneşte calculatorul.

Controlul Regiştrilor supraveghează regiştrii Windows – în acest fel BitDefender poate detecta troienii. BitDefender vă va alerta de fiecare dată când un program încearcă să modifice informațiile din regiştri astfel încât să fie lansat la pornirea Windows.



Alertă regiştri

Puteți vedea programul care încearcă să modifice regiştrii Windows.

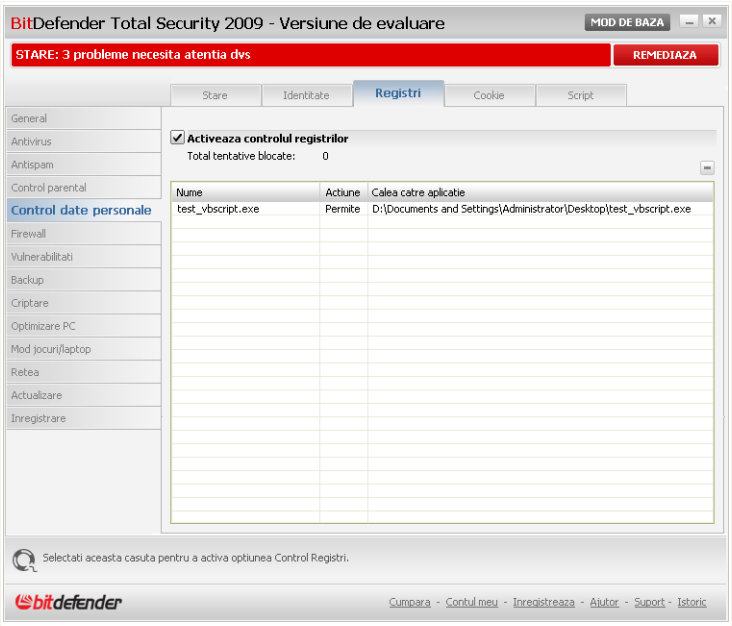
Dacă nu recunoaşteți programul şi acesta pare suspect, faceți clic pe **Blochează** pentru a-l împiedica să modifice regiştrii Windows. Altfel, faceți clic pe **Permite** pentru a permite modificarea.

Pe baza răspunsului dumneavoastră, o regulă este creată şi listată în tabelul de reguli. Aceeaşi acțiune este aplicată de fiecare dată când acest program încearcă să modifice o cheie de regiştri.

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 regiştrilor, mergeți la **Control date>Regiştri** în modul avansat.



Control regiştri

Puteți vedea listate în tabel regulile create până în momentul de față.

Pentru a şterge o regulă, selectați-o şi faceți clic pe butonul **Şterge**.

18.4. Controlul aplicațiilor de tip cookie

Fişierele cookie sunt foarte comune pe Internet. Ele sunt fişiere mici salvate pe calculatorul dumneavoastră. Paginile web creează aceste fişiere pentru a vă monitoriza activitatea pe Internet şi a salva informații specifice despre dumneavoastră.

În general, fişierele cookie vă fac viața mai uşoară. De exemplu ele ajută site-urile să vă rețină numele şi preferințele, pentru a nu trebui să le introduceți la fiecare vizită.

Dar ele pot fi folosite şi pentru a vă compromite intimitatea, urmărindu-vă obiceiurile de navigare pe Internet.

Aici vă ajută **Controlul fişierelor cookie**. Când este activat, **Controlul fişierelor 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 fişierul cookie.

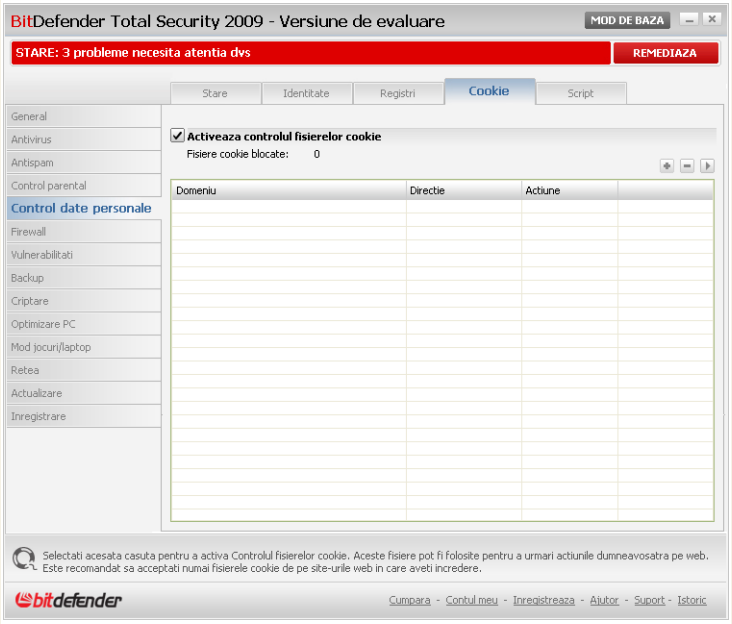
Selectați opțiunea **Reține acest răspuns** şi faceți clic pe **Da** sau **Nu** şi o regulă va fi creată, aplicată şi afişată în lista de reguli. Data viitoare când vă veți conecta la acelaşi site nu veți mai fi notificat.

Aceasta vă va ajuta să alegeți paginile web în care aveți încredere şi pe cele în care nu aveți.

Notă

Din cauza numărului mare de fişiere cookie de pe Internet, **Controlul fişierelor 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 uşoară ca la început.

Pentru a configura Controlul fişierelor cookie, mergeți la **Control date>Cookie** în modul avansat.



Controlul aplicațiilor de tip cookie

Puteți vedea listate în tabel regulile create până în momentul de față.

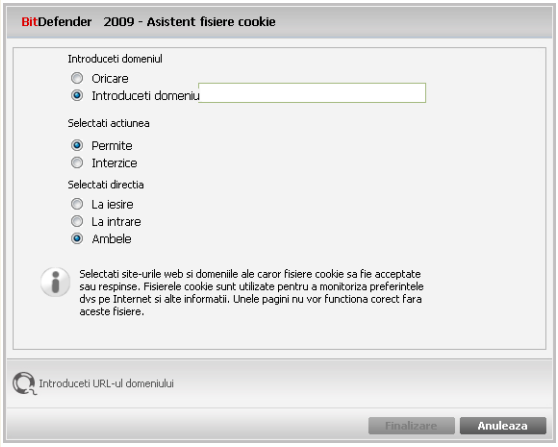
Important
Regulile sunt listate în ordinea priorității începând de sus, adică prima regulă are cea mai mare prioritate. Mutați regulile în sus sau în jos pentru a le schimba prioritatea.

Pentru a şterge o regulă, selectați-o şi faceți clic pe butonul **Şterge**. Pentru a modifica parametrii regulii, faceți dublu-clic pe aceasta şi efectuați modificările dorite în fereastra de configurare.

Pentru a adăuga o regulă manual, faceți clic pe butonul **Adaugă** şi configurați parametrii regulii în fereastra de configurare.

18.4.1. 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	Fişierele cookie de la domeniul respectiv vor fi acceptate.
Interzice	Fişierele cookie de la domeniul respectiv vor fi blocate.

- **Direcție** - selectați direcția traficului.

Tip	Descriere
La ieşire	Regula se aplică fişierelor cookie trimise.
La intrare	Regula se aplică fişierelor cookie recepționate.
Ambele	Regula se va aplica în ambele direcții.

Notă
Puteți accepta fişiere cookie fără a le returna: setați acțiunea **Interzice** şi direcția **La ieşire**.

Faceți clic pe **Finalizare**.

18.5. Control scripturi

Scripturile şi alte coduri cum ar fi elementele ActiveX şi 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 şi le pot citi sau şterge de pe calculatorul dumneavoastră, pot captura parole şi intercepta mesaje cât timp sunteți conectați la Internet. Este recomandat să acceptați conținutul activ doar de la paginile web pe care le cunoaşteți foarte bine şi care sunt de încredere.

BitDefender vă permite să alegeți să permiteți sau să blocați execuția acestor elemente.

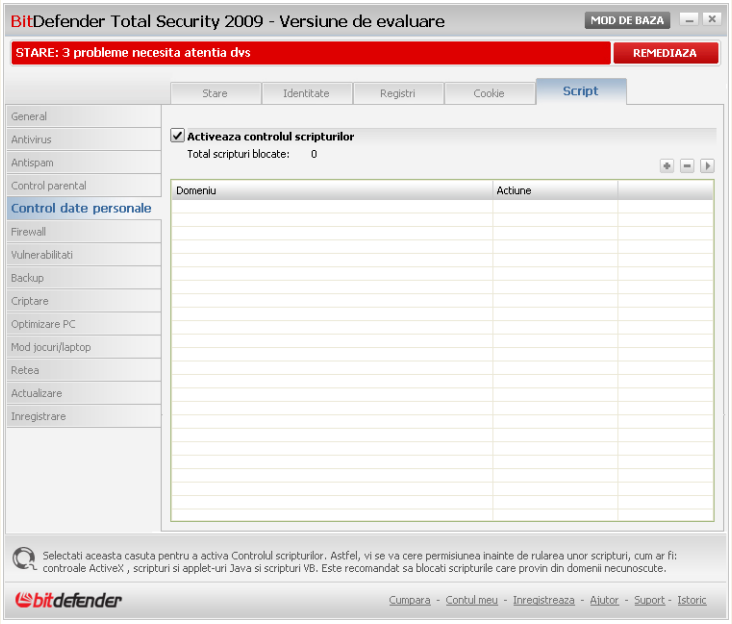
Având **Controlul scripturilor** activat, veți monitoriza adresele web în care aveți încredere şi pe cele în care nu aveți. BitDefender vă va cere permisiunea de fiecare dată când un domeniu încearcă să ruleze un script sau alt conținut activ:

Alertă script

Puteți vedea numele resursei.

Selectați opțiunea **Reține acest răspuns** şi faceți clic pe **Da** sau **Nu** şi o regulă va fi creată, aplicată şi afişată în lista de reguli. Nu veți mai fi notificați data viitoare când acelaşi domeniu încearcă să va trimită conținut activ.

Pentru a configura Controlul scripturilor, mergeți la **Control date>Script** în modul avansat.



Control scripturi

Puteți vedea listate în tabel regulile create până în momentul de față.

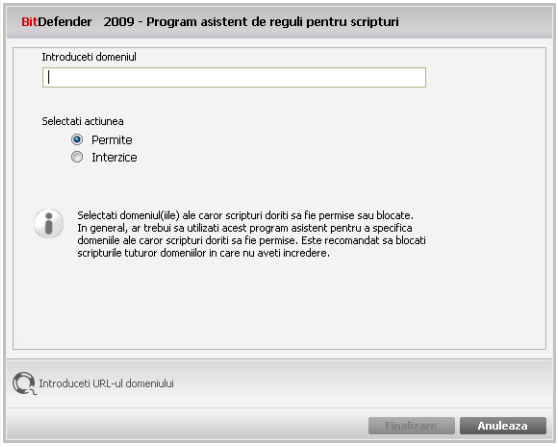
Important
Regulile sunt listate în ordinea priorității începând de sus, adică prima regulă are cea mai mare prioritate. Mutați regulile în sus sau în jos pentru a le schimba prioritatea.

Pentru a şterge o regulă, selectați-o şi faceți clic pe butonul **Şterge**. Pentru a modifica parametrii regulii, faceți dublu-clic pe aceasta şi efectuați modificările dorite în fereastra de configurare.

Pentru a crea o regulă manual, faceți clic pe butonul **Adaugă** şi configurați parametrii regulii în fereastra de configurare.

18.5.1. 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**.

19. Firewall

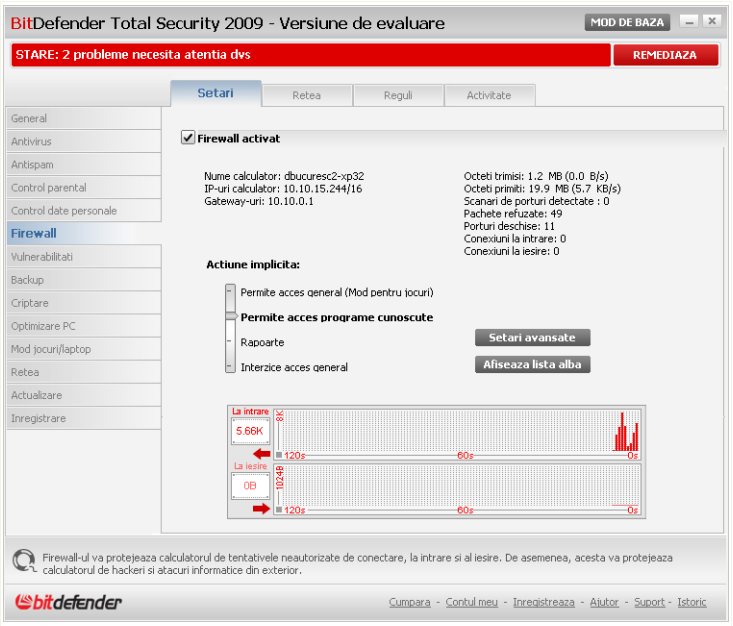
Firewallul vă protejează calculatorul de tentative neautorizate de conectare în ambele direcții (la intrare şi la iesire). Asemenea unui paznic care stă la uşa dumneavoastră, acest modul va supraveghea conexiunea Internet şi va ține o evidență a permisiunilor şi a interdicțiilor de acces la Internet.

Notã
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 maşină pentru a găsi puncte de acces, adesea pregătind un atac) şi să protejeze calculatorul împotriva acestora.

19.1. Setări

Pentru a configura protecția firewall, mergeți la **Firewall>Setări** în modul avansat.



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 şi gateway-ul acestuia. Dacă aveți mai multe plăci de rețea (sunteți conectat la mai multe rețele), veți vedea adresa IP şi gateway-ul configurat pentru fiecare placă de rețea.
- **Statistici.** Puteți vedea statistici variate referitoare la activitatea firewall:
  - numărul de biți trimişi.

- numărul de biți primiți.
- numărul de scanări de porturi detectate şi 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 ieşire active.

Pentru a vedea conexiunile active şi porturile deschise, mergeți la tabul Activitate.

În partea de jos a secțiunii puteți vizualiza statisticile BitDefender referitoare la traficul la intrare şi la ieşire. Graficul arată volumul traficului internet în ultimele două minute.

Notă
Graficul apare chiar dacă modulul **Firewall** este dezactivat.

19.1.1. Setarea acțiunii implicite

În mod implicit, BitDefender permite automat tuturor programelor din lista de programe cunoscute să acceseze rețeaua şi 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 şi permite toate tentativele de trafic care nu se potrivesc niciunei reguli existente, fără niciun avertisment. Această politică nu este recomandată; totuşi, ea poate fi utilă administratorilor de rețea şi pasionaților de jocuri.
Permite cunoscute	Aplică regulile curente şi permite toate tentativele de conectare la ieşire ale programelor cunoscute de BitDefender ca fiind legitime (pe lista albă) fără a solicita

Acțiune implicită	Descriere
	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 şi de transfer de fişiere, precum şi clienți de servere şi programe ale sistemului de operare.
Raport	Aplică regulile curente şi vă consultă în legătură cu tentativele de trafic care nu se potrivesc niciunei reguli existente.
Interzice toate	Aplică regulile curente şi blochează toate tentativele de trafic care nu se potrivesc niciunei reguli existente.

19.1.2. Configurarea setărilor avansate de firewall

Puteți face clic pe **Avansat** 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, şi doriți să poată fi utilizată şi de ceilalți membri ai rețelei.

Împărțirea conexiunii Internet cu membrii rețelelor locale conduce la mărirea consumului de resurse şi implică un anumit grad de risc. De asemenea, vă ocupă unele porturi (cele deschise de membrii ce vă utilizează conexiunea Internet).

- **Monitorizează schimbările în fişierele de program pentru care există reguli firewall** - verifică fiecare aplicație care încearcă să se conecteze la Internet pentru a vedea dacă a fost modificată de când a fost adăugată regula care îi controlează accesul. Dacă aplicația a fost modificată, va apărea o alertă care vă va cere să permiteți sau să refuzați accesul aplicației la Internet.

  În general, aplicațiile sunt modificate în urma actualizărilor. Totuşi, există riscul ca acestea să fie modificate de aplicații malițioase, cu scopul de a infecta calculatorul dumneavoastră precum şi alte calculatoare din rețea.

  Notă
  Vă recomandăm să țineți această opțiune selectată şi să permiteți accesul doar acelor aplicații care vă aşteptați să fi fost modificate după ce a fost creată regula care le controlează accesul.

  Aplicațiile semnate sunt presupuse a fi sigure şi au un grad sporit de securitate. Puteți bifa **Ignoră modificările proceselor semnate** pentru a permite aplicațiilor semnate modificate să se conecteze la Internet fără a primi vreo alertă în legătură cu acest eveniment.

- **Activează notificări wireless** - dacă sunteți conectat la o rețea fără fir (wireless), afişează ferestre informative privind anumite evenimente din rețea (de exemplu, când un calculator nou s-a conectat la rețea).

- **Blochează scanările de porturi** - detectează şi blochează tentativele de a descoperi care porturi sunt deschise.

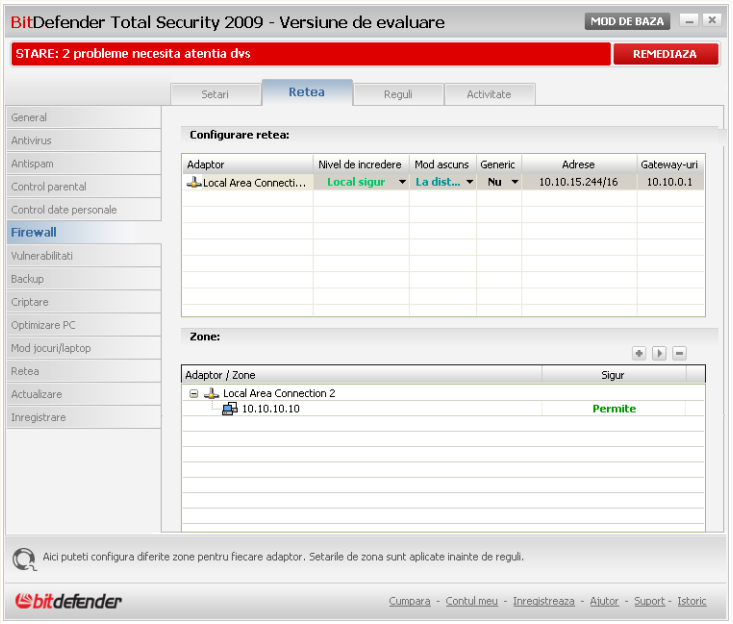
  Scanările de porturi sunt folosite în mod frecvent de hackeri pentru a detecta porturi deschise pe calculatorul dumneavoastră. Dacă este detectat un port vulnerabil, aceştia pot pătrunde în calculatorul dumneavoastră.

- **Reguli automate strice** - creează reguli stricte prin intermediul ferestrei de alertă de firewall. Fiind selectată această opțiune, BitDefender vă va solicita să alegeți acțiunea şi va crea reguli pentru fiecare proces diferit care deschide aplicația care necesită acces la rețea sau Internet.

- **Sistem de detecție a intruziunilor (IDS)** - activează monitorizarea euristică a aplicațiilor care încearcă să acceseze rețeaua şi Internetul.

19.2. Rețea

Pentru a configura setările firewall, mergeți la **Firewall>Rețea** în modul avansat.



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.
- **Tip** - 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.
- **Ascuns** - dacă puteți fi detectat de alte calculatoare.

- **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.

19.2.1. 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 şi procesele BitDefender accesează rețeaua şi Internetul.

Puteți vedea nivelul de încredere configurat pentru fiecare adaptor în tabelul **Configurație rețea**, sub coloana **Tip**. Pentru a modifica nivelul de încredere, faceți clic pe săgeata din coloana **Tip** şi selectați nivelul dorit.

Nivel de încredere	*Descriere*
Încredere deplină	Dezactivează firewallul pentru adaptorul respectiv.
Încredere locală	Permite tot traficul dintre calculatorul dumneavoastră şi 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 şi calculatoarele din rețeaua locală, permițând în acelaşi timp accesul la Internet. Acest nivel de încredere este setat automat pentru rețele fără fir (wireless) nesecurizate.
Blocat	Blochează complet traficul de rețea şi Internet prin adaptorul respectiv.

19.2.2. Configurarea modului ascuns

În modul ascuns, calculatorul dumneavoastră este ascuns față de aplicații periculoase şi de hackeri din rețea sau din Internet. Pentru a configura modul ascuns, faceți clic pe săgeata din coloana **Ascuns** şi 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 şi detecta calculatorul dumneavoastră.
La distanță	Calculatorul dumneavoastră nu poate fi detectat din Internet. Utilizatorii din rețeaua locală pot da ping şi detecta calculatorul dumneavoastră.

19.2.3. Configurarea setărilor generice

Dacă se schimbă adresa IP a unui adaptor de rețea, BitDefender va modifica automat şi nivelul de încredere. Dacă doriți să păstrați acelaşi nivel de încredere, faceți clic pe săgeata din coloana **Generic** şi selectați **Da**.

19.2.4. Zone de rețea

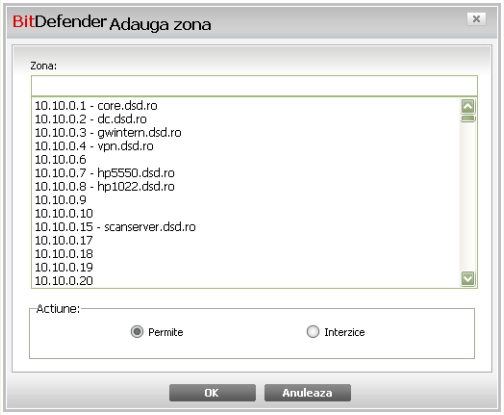
Puteți adăuga calculatoare blocate sau permise pentru un anumit adaptor.

O zonă de încredere este un calculator în care aveți deplină încredere. Tot traficul dintre calculatorul dumneavoastră şi 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** afişează zonele curente de rețea pentru fiecare adaptor în parte.

Pentru a adăuga o zonă, faceți clic pe butonul **Adaugă**.



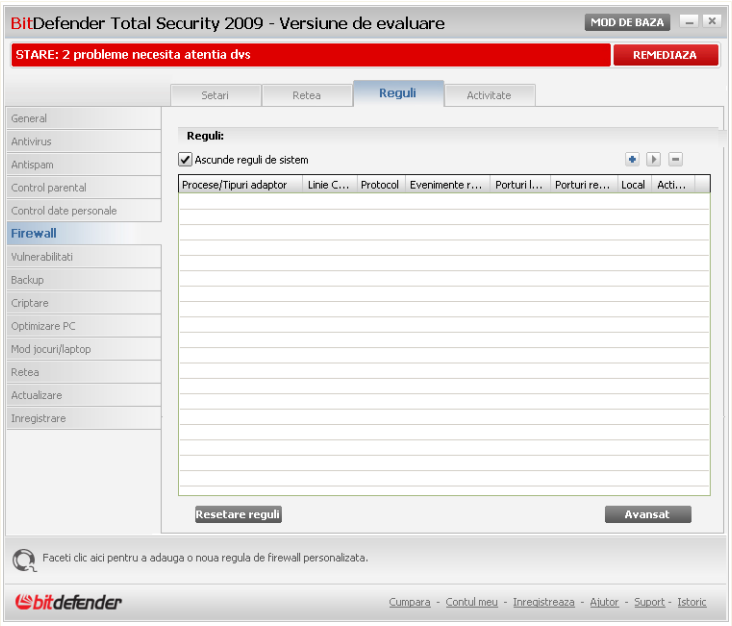
Adăugare zonă

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 şi calculatorul selectat.
   - **Blochează** - pentru a bloca tot traficul dintre calculatorul dumneavoastră şi calculatorul selectat.
3. Faceți clic pe **OK**.

19.3. Reguli

Pentru a administra regulile firewall care controlează accesul aplicațiilor la rețea şi Internet, mergeți la **Firewall>Reguli** în modul avansat.



Reguli firewall

Puteți vedea aplicațiile (procesele) pentru care au fost create reguli firewall. Debifați căsuța **Ascunde regulile de sistem** pentru a vedea şi 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 şi 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 şi 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 şi schimbul de date între două sisteme. TCP garantează livrarea de date şi primirea pachetelor trimise în aceeaşi ordine în care au fost expediate.
UDP	UDP, acronimul pentru User Datagram Protocol, este un protocol bazat pe IP, proiectat pentru performanțe ridicate. Jocurile şi alte aplicații video folosesc adesea acest protocol.
Un număr	Reprezintă un anumit protocol IP (altul decât TCP şi 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 aşteptând 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.

19.3.1. 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 şi portul prin care aplicația încearcă să se conecteze.

Faceți clic pe **Permite** pentru a permite tot traficul (la intrare şi la ieşire) generat de această aplicație de pe calculatorul local către orice destinație, prin protocolul IP respectiv şi 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 şi 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.

19.3.2. Ştergerea regulilor

Pentru a şterge o regulă, selectați-o şi faceți clic pe butonul **Şterge regulă**. Puteți selecta şi şterge mai multe reguli deodată.

Dacă doriți să ştergeți toate regulile create pentru o anumită aplicație, selectați aplicația din listă şi faceți clic pe butonul **Şterge regulă**.

19.3.3. Crearea şi 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 aceşti paşi:

1. Faceți clic pe butonul **Adaugă regulă**. Va apărea fereastra de configurare.

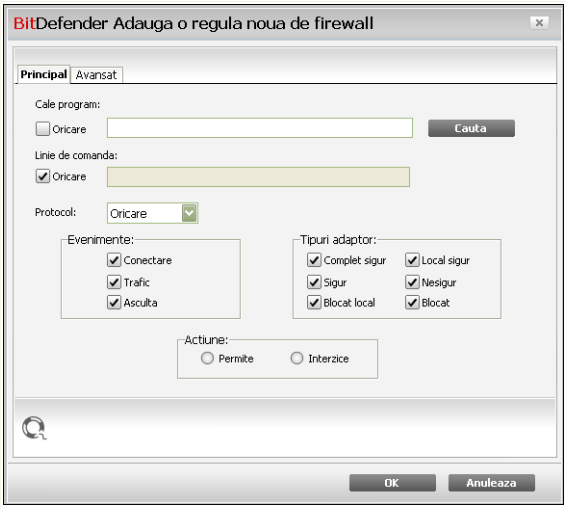
2. Configurați parametrii principali şi pe cei avansați, după cum este nevoie.
3. Faceți clic pe **OK** pentru a adăuga regula.

Modificarea regulilor. Pentru a modifica o regulă existentă, urmați aceşti paşi:

1. Faceți clic pe butonul **Editează regula** sau faceți dublu-clic pe regulă. Va apărea fereastra de configurare.
2. Configurați parametrii principali şi 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** şi 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** şi 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 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:

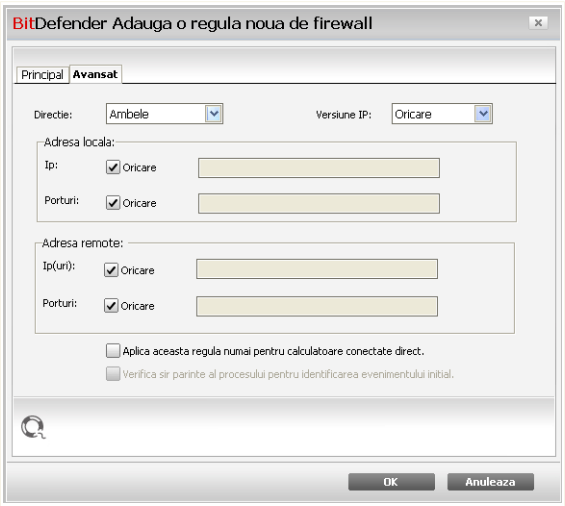
Eveniment	*Descriere*
Conectare	Schimb preliminar de mesaje standard utilizate în cadrul protocoalelor orientate pe conexiune pentru a stabili o conexiune. În cazul protocoalelor orientate pe conexiune, traficul de date dintre două calculatoare apare numai după ce a fost stabilită conexiunea.
Trafic	Schimb de date dintre două calculatoare.
Ascultă	Stare în care o aplicație monitorizează rețeaua aşteptând stabilirea unei conexiuni sau recepționarea unor informații de la o aplicație parteneră.

- **Nivel de încredere.** Selectați nivelele de încredere 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 ieşire	Regula se va aplica doar pentru traficul la ieşire.
La intrare	Regula se aplica doar pentru traficul la intrare.
Ambele	Regula se va aplica în ambele direcții.

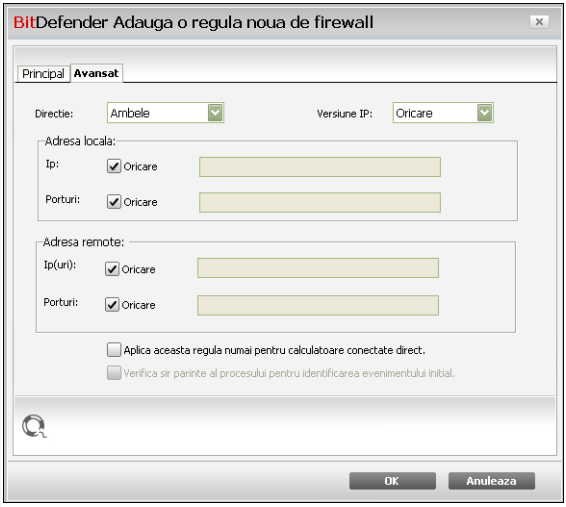
- **Versiune IP.** Selectați din meniu versiunea IP (IPv4, IPv6 sau ambele) căreia i se aplică regula.
- **Adresa locală.** Specificați adresa IP locală şi portul local cărora li se aplică regula după cum urmează:

- Dacă aveți mai multe adaptoare de rețea, puteți debifa căsuța **Oricare** şi introduce o anumită adresă IP.
- Dacă ați selectat TCP sau UDP ca protocol puteți seta un port specific sau o valoare între 0 şi 65535. Dacă doriți ca regula să se aplice tuturor porturilor selectați **Oricare**.

- **Adresa la distanță.** Specificați adresa IP şi portul la distanță cărora li se aplică regula după cum urmează:
  - Pentru a filtra traficul dintre calculatorul dumneavoastră şi un anumit calculator, debifați căsuța **Oricare** şi introduceți adresa IP a acestuia.
  - Dacă ați selectat TCP sau UDP ca protocol puteți seta un port specific sau o valoare între 0 şi 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 şi 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.

19.3.4. 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.

Notã

Atunci când are loc o tentativă de conexiune (la intrare sau la ieşire), BitDefender aplică acțiunea primei reguli care îndeplineşte condițiile conexiunii respective. Din acest motiv, ordinea în care sunt verificate aceste reguli este foarte importantă.

Pentru a şterge o regulă, selectați-o şi faceți clic pe butonul **Şterge regula**.

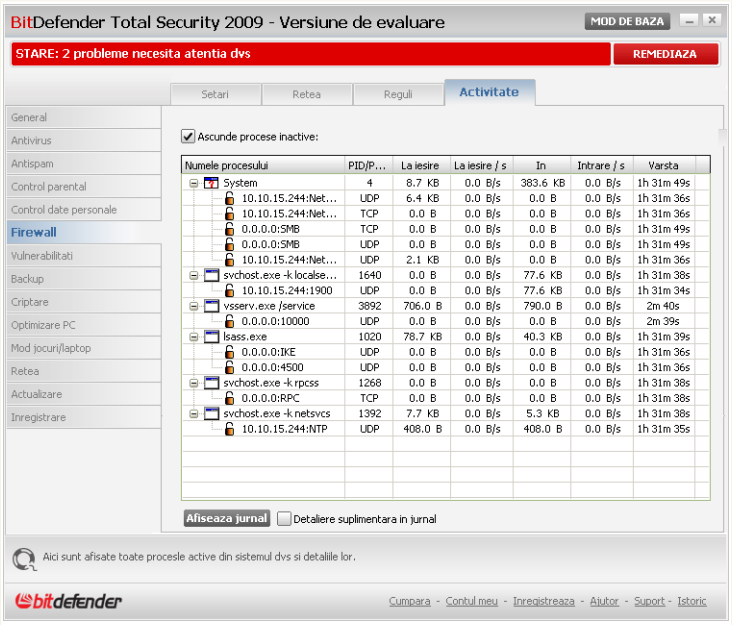
Pentru a modifica o regulă existentă, selectați-o şi faceți clic pe butonul **Editează regula** sau faceți dublu-clic pe regulă.

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.

19.4. Control conexiuni

Pentru a monitoriza activitatea curentă pe rețea / Internet (prin TCP şi UDP) sortată pe aplicații şi pentru a deschide jurnalul BitDefender Firewall, mergeți la **Firewall>Activitate** în modul avansat.



Control conexiuni

Puteți vedea traficul total, sortat după aplicație. Pentru fiecare aplicație, puteți vedea conexiunile şi porturile deschise, precum şi statistici referitoare la viteza traficului la intrare & ieşire şi cantitatea de date trimise / primite.

Dacă doriți să vedeți şi procesele inactive, debifați căsuța **Ascunde procesele inactive**.

Sensul iconițelor este după cum urmează:

- Indică o conexiune deschisă pe calculatorul dumneavoastră.

■ Indică un port deschis pe calculatorul dumneavoastră.

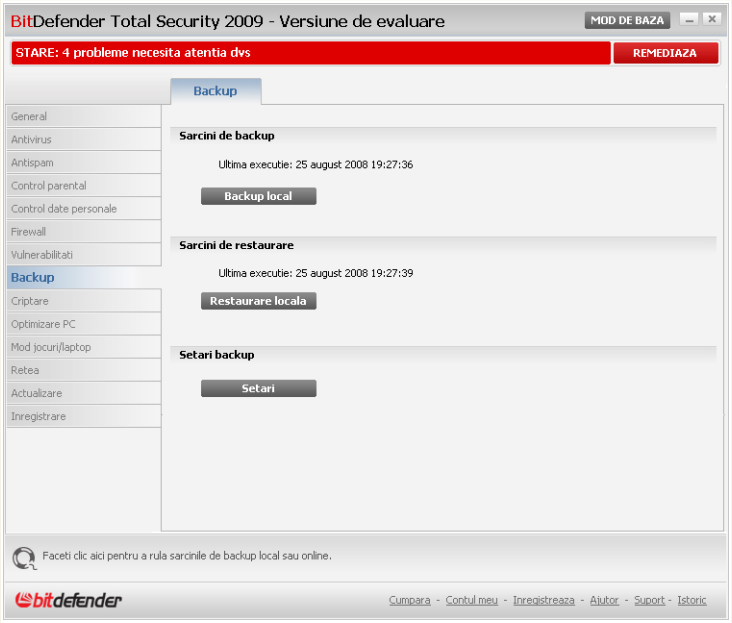
Fereastra prezintă, în timp real, activitatea curentă pe rețea / Internet. Pe măsură ce sunt închise conexiuni şi porturi, statisticile corespunzătoare acestora dispar treptat. Acelaşi lucru se întâmplă tuturor statisticilor unei aplicații care generează trafic sau are porturi deschise atunci când o 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 fişierul jurnal al BitDefender Firewall făcând clic pe **Afişează jurnal**. Fişierul 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**.

20. Sarcini de backup

BitDefender conține un modul de Backup care vă ajută să faceți copii datelor importante de pe calculatorul dumneavoastră. Puteți copia date pe calculatorul dumneavoastră, pe unități mobile sau la locații din rețea pentru a vă asigura că le puteți restaura dacă acest lucru este necesar. Restaurarea datelor dumneavoastră se face uşor.



Sarcini de backup

Următoarele butoane sunt disponibile:

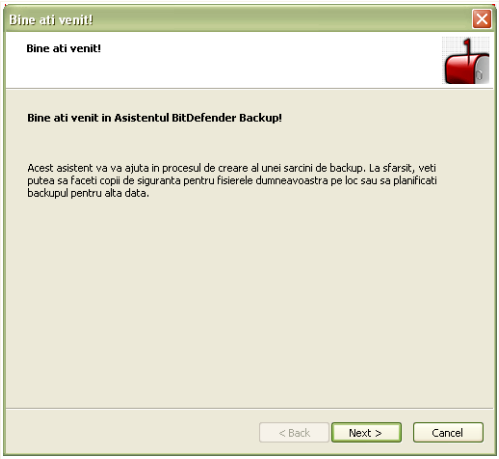
- **Backup local** - lansează un program asistent în cinci paşi care vă ajută să faceți copii de siguranță locale pentru datele dumneavoastră.
- **Restaurare locală** - lansează un program asistent în patru paşi care vă ajută să restaurați copiile de siguranță locale ale datelor dumneavoastră.
- **Setări** - deschide BitDefender Backup, unde puteți seta şi executa operații de backup în detaliu.

20.1. Crearea de copii de siguranță local

Făcând clic pe **Backup local**, veți fi ghidat de către un program asistent prin procesul de creare a unei sarcini de backup local. La sfârşitul acestui proces, veți putea face copii de siguranță pentru fişiere pe loc sau puteți programa produsul să le facă mai târziu.

20.1.1. Pasul 1/5 - Fereastra de întâmpinare

Aceasta este doar o pagină de bun venit.

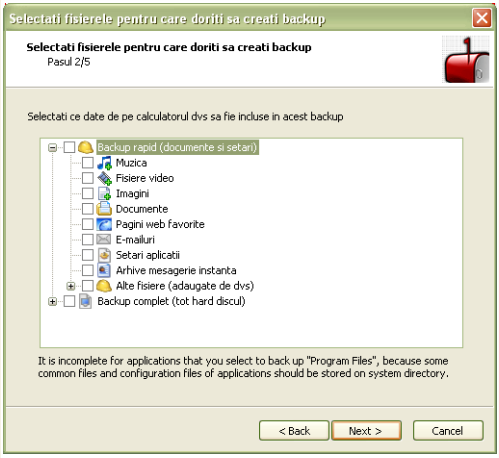


Fereastra de întâmpinare

Faceți clic pe **Înainte**.

20.1.2. Pasul 2/5 - Alegeți la ce să faceți backup

Aici puteți selecta datele de pe calculatorul dumneavoastră la care să faceți copii de rezervă.



Alegeți la ce anume să faceți backup

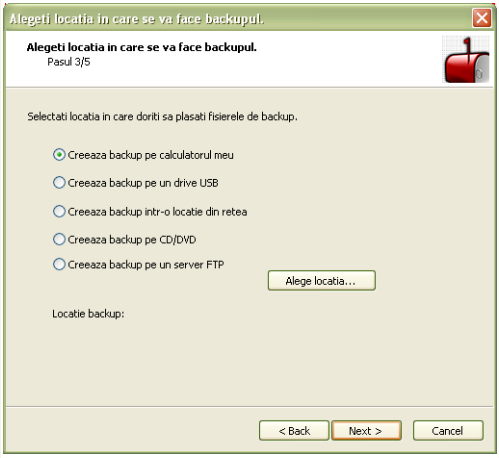
Puteți alege fie **Backup rapid** (muzica, fişierele video, pozele, mesajele email, setările aplicațiilor etc.), fie **Backup complet** (toate partițiile).

Faceți clic pe **Alte fişiere** pentru a adăuga alte fişiere de pe desktopul dumneavoastră la **Backup rapid**. De asemenea, **Backupul complet** poate fi uşor personalizat, selectând directoarele dintr-o anumită partiție pentru care să se facă backup.

Faceți clic pe **Înainte**.

20.1.3. Pasul 3/5 - Alegeți unde să faceți backup

Aici puteți selecta locația copiilor de rezervă.



Alegeți unde să faceți backup

Următoarele opțiuni sunt disponibile:

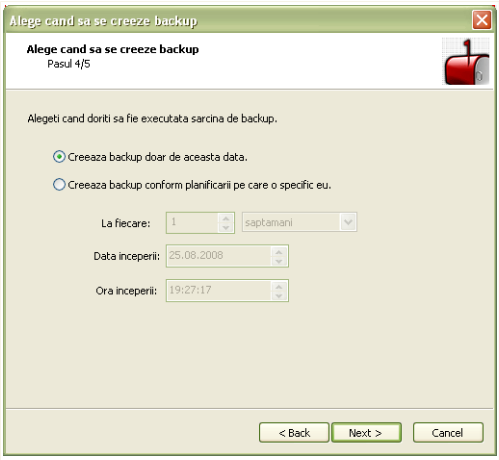
- **Creează backup pe calculator**
- **Creează backup pe un drive USB**
- **Creează backup într-o locație din rețea**
- **Creează backup pe CD/DVD**
- **Creează backup pe un server de FTP**

Dacă decideți să faceți backup pe calculatorul dumneavoastră, pe USB sau pe o locație din rețea, faceți clic pe **Alegeți locație** şi selectați unde să salvați datele.

Faceți clic pe **Înainte**.

20.1.4. Pasul 4/5 - Alegeți când să fie făcut backupul

Aici puteți alege când să fie efectuat backupul.



Alegeți când să fie făcut backupul

Următoarele opțiuni sunt disponibile:

- **Creează backup doar de această dată**
- **Creează backup pe baza programului specificat**

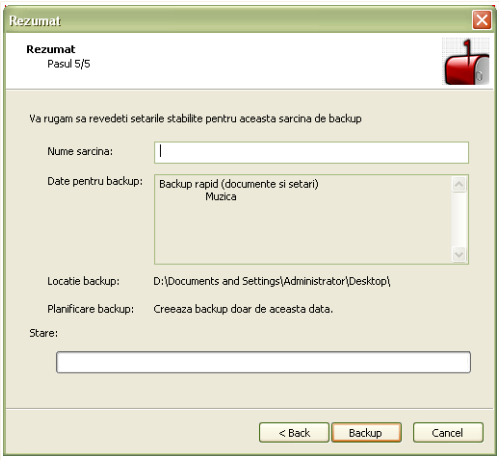
Pentru a face backup la datele dumneavoastră imediat, faceți clic pe **Creează backup doar de această dată**, pentru a programa produsul să facă backup la fişierele dumneavoastră la un moment ulterior, faceți clic pe **Creează backup pe baza programului specificat**.

Dacă selectați **Creează backup pe baza programului specificat**, puteți specifica frecvența cu care să ruleze sarcina programată: zilnic sau săptămânal. De asemenea, puteți specifica momentul şi data la care aceasta să înceapă.

Faceți clic pe **Înainte**.

20.1.5. Pasul 5/5 - Rezumat

Aici puteți revedea setările sarcinii de backup.



Rezumat

Trebuie să introduceți numele sarcinii în câmpul corespunzător.

Faceți clic pe **Backup** dacă sunteți mulțumit de setări.

Faceți clic pe **Finalizare**.

20.2. Restaurarea copiilor de siguranță locale

Făcând clic pe **Backup local**, veți fi ghidat de către un program asistent prin procesul de restaurare a copiilor de siguranță locale.

20.2.1. Pasul 1/4 - Fereastra de întâmpinare

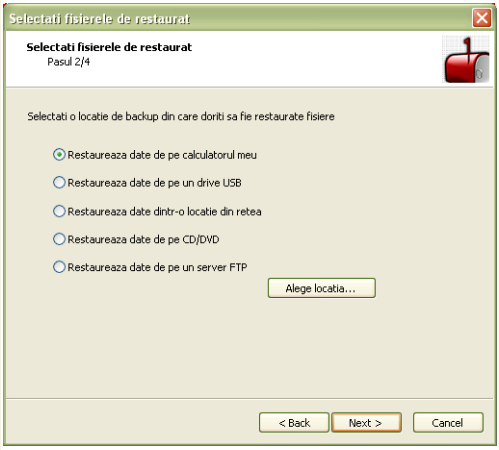
Aceasta este doar o pagină de bun venit.

Fereastra de întâmpinare

Faceți clic pe **Înainte**.

20.2.2. Pasul 2/4 - Alegeți la ce să fie făcut backup

Aici puteți selecta o locație de unde să restaurați fişiere.



Alegeți la ce să fie făcut backup

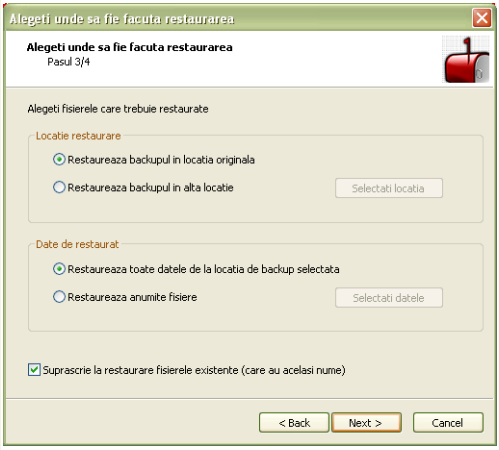
Următoarele opțiuni sunt disponibile:

- **Restaurează date de pe calculator**
- **Restaurează date de pe un drive USB**
- **Restaurează date dintr-o locație din rețea**
- **Restaurează date de pe CD/DVD**
- **Restaurează date de pe un server de FTP**

Faceți clic pe **Înainte**.

20.2.3. Pasul 3/4 - Alegeți locația și fișierele pentru restaurare

Aici puteți alege care fişiere să fie restaurate şi unde doriți să fie restaurate.



Alegeți locația de restaurare și fișierele restaurate

Următoarele opțiuni sunt disponibile:

- **Restaurează backup în locația originală**
- **Restaurează backupul în altă locație**
- **Restaurează toate datele din locația de backup selectată**
- **Restaurează anumite fișiere**
- **Suprascrie la restaurare fișierele existente**

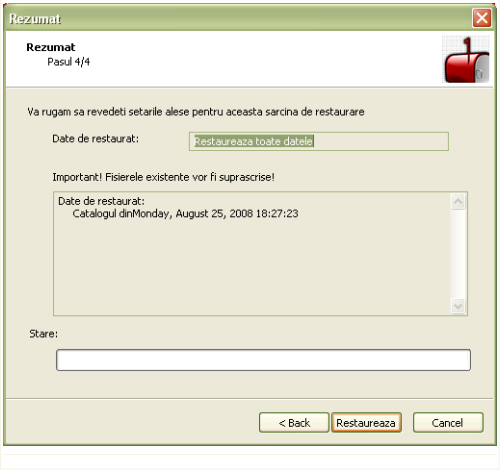
Dacă doriți să restaurați date în altă locație sau doar anumite fișiere, selectați locația și datele făcând clic pe butonul corespunzător.

Pentru a evita suprascrierea fișierului existent la restaurare, debifați căsuța **Suprascrie la restaurare fișierele existente**.

Faceți clic pe **Înainte**.

20.2.4. Pasul 4/4 - Rezumat

Aici puteți revedea setările sarcinii de restaurare.



Faceți clic pe **Restaurează** dacă sunteți mulțumit de setări.

Faceți clic pe **Finalizare**.

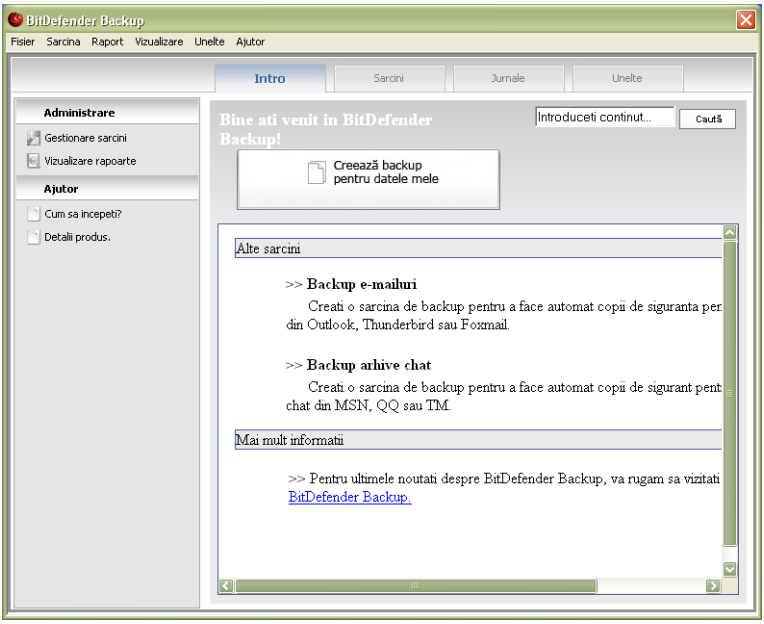
20.3. Opțiuni avansate de backup

Dacă doriți să efectuați operațiuni complexe de creare şi restaurare de copii de siguranță, puteți folosi soluția completă BitDefender Backup. Soluția BitDefender Backup oferă:

- o varietate de opțiuni pentru crearea de copii de siguranță, cum ar fi compresie, criptare, filtrare de fişiere sau setare viteză de backup.
- control avansat asupra restaurării de fişiere (de exemplu, puteți restaura copiile de siguranță create la un anumit moment de timp).
- posibilități de planificare avansată (de exemplu, puteți alege ca sarcina de creare a copiilor de siguranță să fie executată la pornirea sistemului sau atunci când calculatorul este neutilizat mai mult timp).
- o secțiune de jurnale care vă ajută să monitorizați operațiunile de creare şi restaurare de copii de siguranță efectuate şi să rezolvați eventualele erori.

În această secțiune, vă sunt furnizate informații detaliate despre interfața grafică şi capabilitățile oferite de BitDefender Backup.

Pentru a deschide BitDefender Backup, faceți clic pe **Setări backup**.

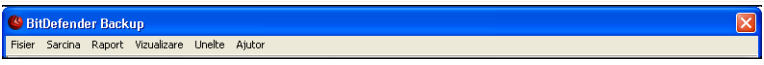


BitDefender Backup

Există două metode de a configura şi executa operații de creare de copii de siguranță. Puteți fie să accesați **bara de meniuri** din partea superioară, fie să faceți clic pe un anumit tab din **bara de navigare**.

20.3.1. Bara de meniuri

Puteți utiliza şase meniuri pentru a executa funcțiile oferite de soluția de backup BitDefender.



Bara de meniuri

Fişier

- **Creează sarcină nouă:** afişează o căsuță de dialog care permite crearea unei noi sarcini de backup sau a unei alte sarcine.
- **Deschide set de backup:** afişează o căsuță de dialog care permite deschiderea unui set de backup sau a unui catalog pentru restaurare.
- **Ieşire:** închide secțiunea BitDefender backup.

Sarcină

- **Backup:** execută sarcina selectată. Dacă sunt mai multe sarcini selectate, atunci toate vor fi executate.
- **Restaurează fişier:** restaurează sarcina selectată. Dacă sunt mai multe sarcini selectate, atunci toate vor fi executate.
- **Restaurează după dată:** restaurează sarcina selectată de la un anumit moment. Dacă sunt mai multe sarcini selectate, atunci toate vor fi executate.
- **Planificare:** creează programul de executare a sarcinii sau modifică programul existent.
- **Şterge planificare:** şterge programul de executare a sarcinii planificate.
- **Şterge:** şterge sarcina selectată. Dacă sunt mai multe sarcini selectate, atunci toate vor fi şterse.
- **Şterge tot:** şterge toate sarcinile din fereastra Sarcini.
- **Cautare în destinație:** permite vizualizarea datelor din destinația sarcinii selectate.
- **Modifică opțiuni:** modifică opțiunile sarcinii selectate.
- **Proprietăți:** permite modificarea proprietăților sarcinii selectate, incluzând sursa datelor, numele sarcinii, destinația sarcinii etc.

Raport

- **Afişează rapoarte:** dacă sarcina selectată are setări de securitate, această opțiune permite examinarea conținutului raportului.
- **Salvează ca:** salvează conținutul raportului selectat într-un fişier specificat.
- **Tipăreşte:** scoate la imprimantă conținutul raportului selectat.
- **Şterge tot:** şterge conținutul raportului de sarcină selectat.
- **Actualizează:** actualizează conținutul raportului de sarcină selectat.

Vizualizare

- **Intro:** dacă fereastra Intro nu este deja afişată, această opțiune vă permite să o deschideți.
- **Sarcini:** dacă fereastra Sarcini nu este deja afişată, această opțiune vă permite să o deschideți.
- **Jurnale:** dacă fereastra Jurnale nu este deja afişată, această opțiune vă permite să o deschideți.

- **Unelte:** dacă fereastra Unelte nu este deja afişată, această opțiune vă permite să o deschideți.
- **Afişează bara de meniuri:** ascunde bara de meniuri. Pentru a o afişa, apăsați tasta **ALT**.
- **Afişează grilă:** afişează sau ascunde grila. Aceasta se aplică ferestrelor Jurnal şi Sarcini.

Unelte

- **Asistent backup:** lansează programul asistent de backup.
- **Asistent restaurare:** lansează programul asistent de restaurare.
- **Inscripționare:** porneşte un utilitar de inscripționare CD/DVD/ISO sau de administrare a operației de inscripționare.
  - **Inscripționare CD/DVD**
  - **Inscripționare fişiere ISO**
  - **Afişează informații inscripționare**
- **Exportă toate sarcinile:** exportă toate sarcinile create într-un fişier specificat.
- **Importă sarcini:** importă sarcini dintr-un fişier `.JOB`, `.TXT` sau `.XML`.
- **Exportă jurnal:** exportă jurnale într-un fişier `.TXT` sau `.XML`.
  - într-un fişier `TXT`
  - într-un fişier `XML`
- **Importă jurnal:** importă jurnale dintr-un fişier `.TXT` sau `.XML`.
  - dintr-un fişier `TXT`
  - dintr-un fişier `XML`
- **Opțiuni:** modifică opțiunile globale de backup.
  - **General**
  - **Rapoarte & Jurnal**
  - **Planificare sarcină**

Ajutor

- **Conținut Ajutor:** deschide documentația electronică.
- **Caută:** permite căutarea în conținutul documentației electronice după cuvinte selectate sau introduse.
- **Pagina web a BitDefender:** permite accesul către pagina web a BitDefender, precum şi către paginile acesteia unde puteți căuta ştiri BitDefender şi suport online.
- **Despre BitDefender Backup:** afişează simbolul de copyright, versiunea şi informații referitoare la ediția BitDefender Backup.

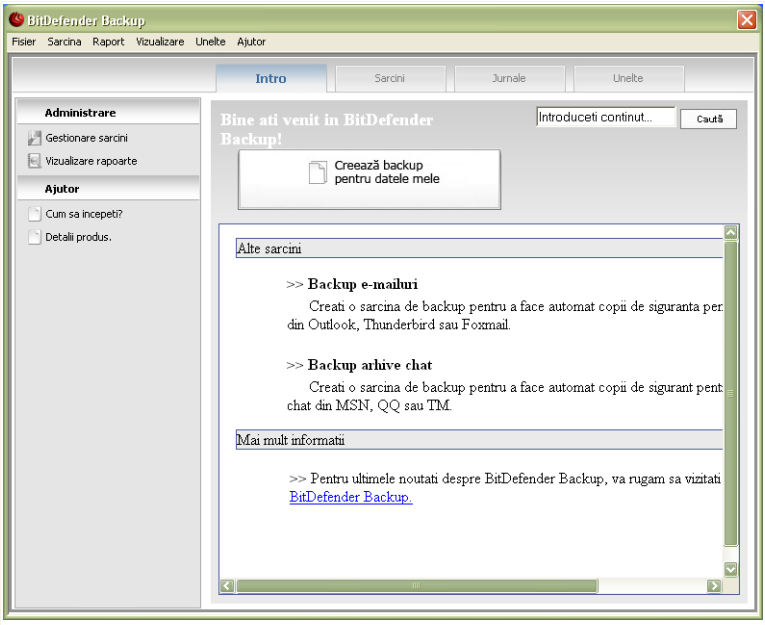
20.3.2. Bara de navigare

Bara de navigare, afişată în partea superioară a ferestrei principale, sub **bara de meniuri**, permite accesul către patru secţiuni:

- **Intro**
- **Sarcini**
- **Jurnale**
- **Unelte**

Intro

Secţiunea **Intro** vă ajută să creaţi cu uşurinţă copii de siguranţă pentru e-mailuri, arhive de chat şi date.



Intro

Puteţi comuta pe fereastra **Intro** folosind una dintre următoarele metode:

- Faceți clic pe **Intro** în **bara de navigare**.
- Faceți clic pe **Vizualizare** în **bara de meniuri** şi selectați **Intro**.
- Utilizați o scurtătură apăsând **CTRL+Alt+S**.

Pentru a face copii de siguranță pentru documentele, pozele, mesajele şi arhivele de chat importante, în timpul aceleeaşi sarcini, faceți clic pe butonul **Backup date** şi urmați procedura în trei paşi.

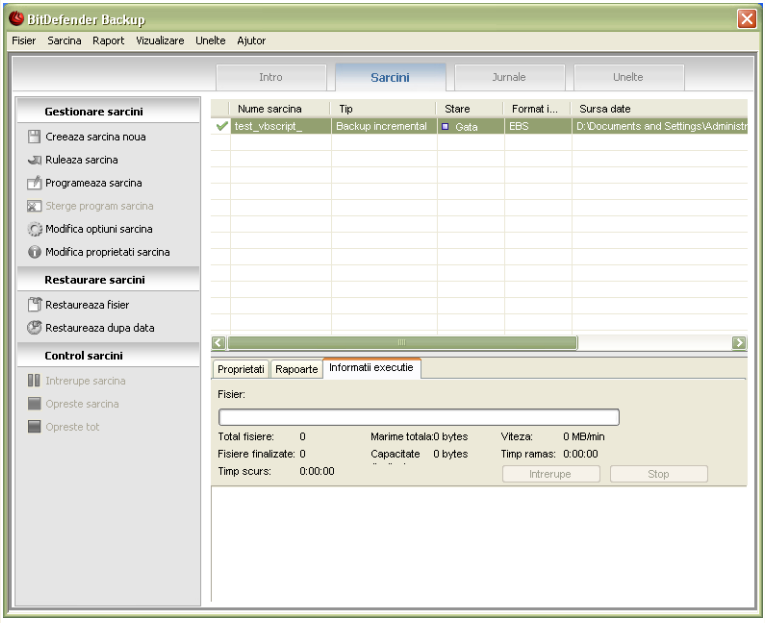
Pentru a face copii de siguranță doar pentru e-mailurile dumneavoastră, faceți clic pe butonul **Backup e-mailuri** şi urmați procedura în trei paşi.

Pentru a face copii de siguranță doar pentru arhivele dumneavoastră de chat, faceți clic pe butonul **Backup arhive chat** şi urmați procedura în trei paşi.

Notă
Procedura în trei paşi este descrisă şi în secțiunea Creează sarcină nouă.

Sarcini

Fereastra **Sarcini** este utilizată pentru a vedea şi gestiona sarcinile de backup, pentru a vedea proprietățile şi rapoartele sarcinilor precum şi pentru a monitoriza viteza de executare a acestora. Fereastra **Sarcini** permite verificarea proprietăților sarcinilor şi starea curentă, modificarea setărilor sarcinilor precum şi executarea de sarcini de backup şi restaurare.



Sarcini

Puteți comuta pe fereastra **Sarcini** folosind una dintre următoarele metode:

- Faceți clic pe **Sarcini** în **bara de navigare**.
- Faceți clic pe **Vizualizare** în **bara de meniuri** şi selectați **Sarcini**.
- Utilizați o scurtătură apăsând **CTRL+Alt+M**.

În partea stângă, veți vedea o listă cu linkuri pentru operare rapidă, după cum urmează:

Gestionare sarcini

- **Creeaza sarcină nouă**
- **Rulează sarcina**
- **Programează sarcina**
- **Şterge planificare sarcină**
- **Modifică opțiuni sarcină**
- **Modifică proprietăți sarcină**

Restaurare sarcini

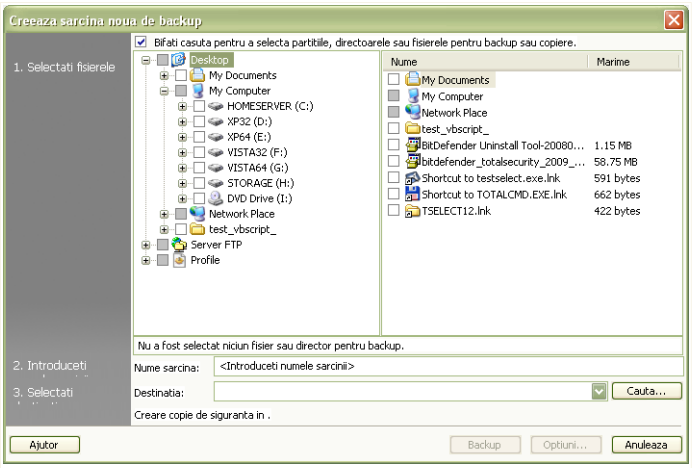
- **Restaurează fişier**
- **Restaurează după dată**

Control sarcini

- **Întrerupe sarcină**
- **Opreşte sarcină**
- **Opreşte tot**

Creează sarcină nouă

Pentru a face copii de siguranță pentru documentele, pozele, mesajele şi arhivele de chat importante, în timpul aceleeaşi sarcini, faceți clic pe butonul **Creează sarcină nouă** şi urmați cei trei paşi.



Creează sarcină nouă

1. Faceți clic pe căsuță pentru a selecta partiții, directoare şi fişiere pentru backup.

   Atunci când selectați un obiect în fereastra din partea stângă, conținutul acestuia va fi afişat în fereastra din partea dreaptă pentru a vă permite o selecție mai precisă.
2. Introduceți un nume pentru sarcina de backup sau păstrați numele implicit.

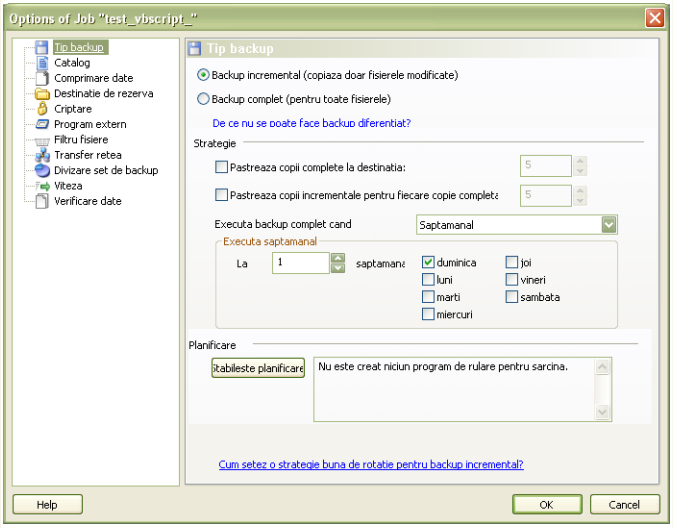
   Numele implicit al sarcinii este generat automat atunci când sunt selectate fişiere sau directoare pentru backup, dar acesta poate fi modificat.

3. Faceți clic pe **Caută** pentru a alege unde să fie salvată sarcina de backup.

Notă
Nu uitați să faceți clic pe **Backup** pentru a începe sau pe **Anulare** pentru a anula. Pentru setări detaliate, faceți clic pe **Opțiuni**.

Căsuța de dialog a opțiunilor de backup

În căsuța de dialog **Opțiuni**, există câteva sub-opțiuni.



Căsuța de dialog a opțiunilor de backup

Tip backup

Soluția de backup BitDefender suportă două tipuri de backup.

- **Backup complet:** face un backup complet al sursei selectate în setul de backup, la locația specificată. Atunci când se execută un backup complet, nu vor fi copiate doar datele modificate, ci întreaga sursă.
- **Backup incremental:** atunci când este executat prima dată, backupul incremental este identic cu backupul complet, deoarece se copiază toate datele din sursă în setul de backup la destinația specificată. După aceea însă, se face

backup doar fişierelor modificate sau celor nou create. De fiecare dată când este executat un backup incremental, este creat un catalog de backup.

De asemenea, backupul incremental şi cel complet pot fi combinate într-un **Backup alternativ**. De exemplu, puteți seta un backup incremental pentru sarcină şi un backup complet o dată pe săptămână, să zicem sâmbăta. Acesta lucru se face în felul următor: selectați **Săptămânal** din meniu, 1 din câmpul **La fiecare săptămâni** şi bifați Duminică. Acest backup complet executat duminica va înlocui toate backupurile anterioare şi va reprezenta baza de la care porneşte noul backup incremental.

Catalog

Este utilizat pentru a indexa informațiile despre fişierele fiecărui backup şi reprezintă baza backupului incremental şi a procesului de restaurare. Catalogul (`*.ecs`) conține o serie de cataloage reprezentând un index al tuturor fişierelor şi directoarelor din setul de backup. Un astfel de index include informații despre momentul la care s-a făcut backupul, directorul de backup, nume şi proprietăți de fişiere. Datele pot fi restaurate din setul de cataloage.

Numele unui catalog este generat automat după destinația sarcinii. Pentru a modifica catalogul unei sarcini, urmați paşii:

1. Faceți clic pe **Catalog**.
2. Introduceți un nume de fişier în câmpul corespunzător.
3. Faceți clic pe **Caută** pentru a selecta directorul în care să fie salvate fişierele setului de cataloage.
4. Faceți clic pe **OK**.

Comprimare date

BitDefender Backup permite comprimarea şi salvarea datelor în setul de backup la executarea operației de backup pentru a salva spațiu. Acesta suportă Comprimare rapidă, Comprimare standard, Comprimare puternică. De exemplu, pentru a porni o comprimare standard la o rată şi o viteză de comprimare medie, urmați aceşti paşi:

1. Faceți clic pe **Comprimare date**.
2. Faceți clic pe **Comprimare standard**.
3. Faceți clic pe **OK**.

Destinație de rezervă

BitDefender Backup permite relocarea setului de backup către o destinație diferită. În acest caz, executarea operației de backup va continua, chiar dacă o anumită destinație nu are suficient spațiu liber.

Puteți adăuga una sau mai multe destinații pentru a continua backupul, le puteți modifica sau chiar şterge, utilizând una dintre metodele următoare:

1. Faceți clic pe **Destinație de rezervă**.
2. Faceți clic pe **Adaugă** pentru a selecta o nouă destinație pentru copia de rezervă.
3. Faceți clic pe **Editează** pentru a modifica destinația de backup selectată.
4. Faceți clic pe **Şterge** pentru a şterge destinația de backup selectată.
5. Faceți clic pe **Şterge tot** pentru a şterge toate destinațiile de backup.
6. Faceți clic pe **OK**.

Criptare

BitDefender Backup asigură o protecție adițională a datelor criptându-le înainte de a le salva la setul de backup. Setările de securitate ale unei sarcini includ şi protecția prin parolă.

Pentru a cripta datele înainte de backup, urmați aceşti paşi:

1. Faceți clic pe **Criptare**.
2. Selectați un tip de criptare din meniul drop-down.
3. Introduceți parola în câmpul corespunzător.
4. Reintroduceți parola în câmpul corespunzător.
5. Faceți clic pe **OK**.

Program extern

Sarcina poate rula altă comandă înainte sau după backup, iar comanda poate fi `.exe`, `.com` sau `.bat`, sau un anumit tip de eveniment, cum ar fi "închide calculatorul la sfârşitul backupului".

Pentru a executa comanda la pornirea backupului, urmați aceşti paşi:

1. Faceți clic pe **Program extern**.
2. Selectați opțiunea **Înainte de execuția sarcinii**.
3. Faceți clic pe **Caută** pentru a selecta fişierele de comandă care să fie executate.
4. Faceți clic pe **OK**.

Pentru a executa o comanda la sfârşitul backupului, urmați aceşti paşi:

1. Faceți clic pe **Program extern**.
2. Selectați opțiunea **După executarea sarcinii**.
3. Faceți clic pe **Caută** pentru a selecta fişierele de comandă care să fie executate.
4. Sau faceți clic pe **Oprire calculator** la sfârşitul backupului.
5. Sau faceți clic pe **Repornire calculator** la sfârşitul backupului.
6. Sau faceți clic pe **Ieşire din cont** la sfârşitul backupului.
7. Faceți clic pe **OK**.

Notă
Dacă doriți ca setările să funcționeze chiar şi în cazul unui eşec al operației de backup, bifați **Execută programul extern chiar dacă execuția sarcinii a eşuat**.

Filtru fişiere

BitDefender Backup oferă o funcție avansată de filtrare pentru a exclude sau include anumite fişiere, tipuri de fişiere sau directoare, pentru a economisi spațiul de stocare şi pentru a îmbunătăți viteza de backup.

Pot fi filtrate tipuri de fişiere urmând aceşti paşi:

1. Faceți clic pe **Filtru fişiere**.
2. Faceți clic pe **Filtrare după tip**.
3. Excludeți sau includeți tipuri de fişiere, din căsuța de dialog, bifând opțiunile **Include doar tipurile de fişiere selectate** sau **Exclude tipurile de fişiere selectate**.
4. Dacă este necesar, introduceți un alt tip de fişier în câmpul **Tip personalizat**, dar asigurați-vă că folosiți un format de tip **.** abc. Utilizați **,** (virgula) ca separator atunci când introduceți mai multe tipuri personalizate. Adăugați o scurtă descriere în câmpul corespunzător.
5. Faceți clic pe **OK**.

Pot fi filtrate fişiere urmând aceşti paşi:

1. Faceți clic pe **Filtru fişiere**.
2. Faceți clic pe **Filtrare fişiere**.
3. Excludeți sau includeți anumite fişiere, din căsuța de dialog, bifând opțiunile **Include doar fişierele desemnate de regulă** sau **Exclude fişierele desemnate de regulă**.
4. Faceți clic pe **Caută** şi selectați fişierul. Calea către locația fişierului va fi adăugată automat în câmpul **Se aplică următoarelor directoare**. Pentru a include sau exclude fişierul indiferent de locația sa, faceți clic pe **Se aplică tuturor directoarelor**.
5. Faceți clic pe **OK**.

Pot fi filtrate directoare urmând aceşti paşi:

1. Faceți clic pe **Filtru fişiere**.
2. Faceți clic pe **Filtrare directoare**.
3. Excludeți sau includeți anumite directoare, din căsuța de dialog, bifând opțiunile **Include doar directoarele desemnate de regulă** sau **Exclude directoarele desemnate de regulă**.
4. Faceți clic pe **Caută** şi selectați directorul. Calea către director va fi adăugată automat în câmpul **Se aplică următoarelor directoare**. Pentru a include sau

exclude directoare indiferent de locația lor, faceți clic pe **Se aplică tuturor directoarelor**.

5. Faceți clic pe **OK**.

Filtrele pot fi modificate urmând aceşti paşi:

1. Faceți clic pe **Filtru fişiere**.
2. Faceți clic pe filtrul pe care doriți să îl modificați şi faceți clic pe **Editează**.
3. Modificați opțiunile dumneavoastră în căsuța de dialog.
4. Faceți clic pe **OK**.

Filtrele pot fi şterse urmând aceşti paşi:

1. Faceți clic pe **Filtru fişiere**.
2. Faceți clic pe filtrul pe care doriți să îl ştergeți şi apoi pe **Şterge**.
3. Sau faceți clic pe direct pe **Şterge tot** pentru a şterge toate filtrele.
4. Faceți clic pe **OK**.

Transfer rețea

BitDefender Backup permite executarea de operații de backup şi restaurare a datelor partajate din rețea. Dacă rețeaua nu este disponibilă, se va încerca executarea backupului în mod regulat. Pentru a specifica frecvența şi numărul de încercări de a face backup, urmați aceşti paşi.

1. Faceți clic pe **Transfer rețea**.
2. Faceți clic pe **Când eşuează citirea fişierelor din rețea din cauza deconectării, încearcă reconectarea la rețea**.
3. Introduceți intervalul de timp (în secunde) la care să se încerce din nou executarea operației de backup.
4. Introduceți numărul de încercări de a executa operația de backup.
5. Faceți clic pe **OK**.

Notă

Pentru a evita un surplus excesiv de informații referitoare la erori de rețea, faceți clic pe **Nu este generat niciun raport de eroare atunci când rețeaua nu este disponibilă**.

Divizare set de backup

Setul de backup generat poate fi divizat în mai multe seturi de backup, astfel încât operația de backup să poată fi executată normal chiar şi atunci când destinația sau sistemul de fişiere este limitat. BitDefender Backup oferă două metode de divizare: auto-divizarea şi divizarea bazată pe mărime.

Setările de divizare ale sarcinii pot fi modificate după cum urmează:

1. Faceți clic pe **Divide set de backup**.
2. Selectați **Divizare automată după spațiul destinației**.

3. Sau selectați **Specificați mărimea pentru divizare** şi alegeți mărimea dorită din meniu.
4. Faceți clic pe **OK**.

Viteză

BitDefender Backup suportă trei tipuri de viteză. Cu cât viteza este mai mare, cu atât va fi procesorul mai solicitat.

Viteza de backup poate fi specificată urmând aceşti paşi.

1. Faceți clic pe **Viteză**.
2. Selectați viteza **maximă**, **medie** sau **minimă**.
3. Faceți clic pe **OK**.

Verificare date

Pentru a vă asigura că datele de backup sunt întotdeauna în siguranță, urmați aceşti paşi:

1. Faceți clic pe **Verificare date**.
2. Faceți clic pe **Verifică datele în procesul de backup**.
3. Faceți clic pe **OK**.

Rulează sarcina

O dată ce sarcina a fost creată, operația de backup este executată automat. Totuşi, puteți accesa fereastra **Sarcini** pentru a executa operația de backup selectând sarcina creată şi făcând clic în meniu pe **Rulează sarcina**.

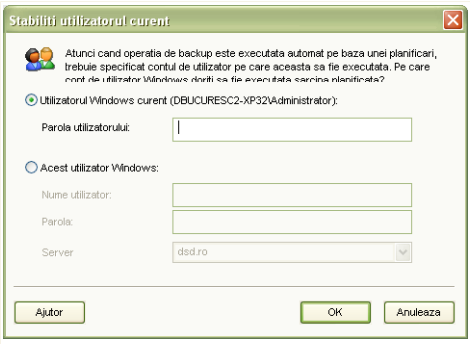
Pentru a primi detalii legate de backup la restaurarea fişierelor, trebuie să introduceți o scurtă descriere în fereastra care se va deschide. Faceți clic pe **Anulare** pentru a ignora fereastra sau pe **OK** pentru a continua. Sarcina de backup poate fi anulată, de asemenea, făcând clic pe butonul **Anulare backup**.

Notă

Pentru mai multe informații, puteți accesa taburile **Proprietăți**, **Rapoarte** şi **Informații execuție** din fereastra de stare.

Planifică sarcina

Aici puteți programa sarcina de backup să ruleze la un moment convenabil. Puteți programa sarcina să fie executată zilnic, săptămânal, lunar sau la un moment dat (de exemplu, la pornirea sistemului). Programarea sarcinilor reprezintă baza backupului automat.



Planifică sarcina

În cazul în care calculatorul dumneavoastră face parte dintr-un domeniu, o serie de paşi adiționali sunt necesari pentru a programa o sarcină.

1. Selectați sarcina şi apoi faceți clic pe **Planifică sarcina**.
2. Va apărea căsuța **Stabiliti utilizatorul curent**. Dacă sunteți utilizator în domeniu, introduceți parola domeniului.
3. Altfel, selectați **Acest utilizator Windows**.
4. Introduceți numele de utilizator, parola şi numele serverului de domeniu.
5. Faceți clic pe **OK**.

O dată ce ați setat utilizatorul curent, BitDefender Backup va afişa căsuța de dialog **Program** pentru a putea seta un timp convenabil pentru executarea sarcinii.

Aici puteți specifica frecvența cu care este rulată sarcina programată: zilnic, săptămânal, lunar, o singură dată, la pornirea sistemului, la logare, atunci când calculatorul nu este folosit. Dacă sarcina este planificată zilnic, săptămânal, lunar sau o singură dată, puteți specifica momentul lansării în execuție. De asemenea, puteți selecta frecvența cu care să fie rulată sarcina (exprimată prin numărul de zile sau săptămâni, ziua lunii sau data). O altă setare posibilă este durata (în minute) perioadei în care nu este utilizat calculatorul după care să fie pornită sarcina programată.

De asemenea, este posibilă configurarea mai multor programe de rulare pentru o sarcină, făcând clic pe **Afişează programe multiple**. Făcând clic pe **Avansat** puteți seta opțiuni adiționale pentru programarea sarcinii. De exemplu, puteți specifica data de început şi pe cea de sfârşit a sarcinii.

Pentru o configurare mai detaliată a programului, faceți clic pe tabul **Setări**. Sunt disponibile trei opțiuni.

- **Sarcină planificată finalizată**
  - Şterge sarcina dacă nu este programată să ruleze din nou.

    Această sarcină este utilă pentru sarcinile programate să ruleze o singură dată.
  - Opreşte sarcina dacă rulează de mai mult de:

    Specificați după cât timp de la lansarea în execuție ar trebui oprită sarcina.
- **Inactivitate**
  - Lansează sarcina în execuție doar dacă perioada de inactivitate a calculatorului este de cel puțin:

    Specificați cât timp (în minute) trebuie să treacă fără a fi utilizate mouse-ul sau tastatura pentru a lansa în execuție sarcina planificată.
  - Dacă perioada de inactivitate a calculatorului este mai mică decât cea specificată, încearcă încă:

    Specificați pentru cât timp (în minute) să fie verificată perioada de inactivitate a calculatorului.
  - Opreşte sarcina atunci când calculatorul este utilizat.

    Specificați dacă ar trebui oprită sarcina dacă începeți să utilizați calculatorul în timp ce sarcina rulează.
- **Gestionarea consumului de curent**
  - Nu lansa sarcina atunci când calculatorul funcționează pe baterii.

    Specificați dacă sarcina nu trebuie să ruleze atunci când calculatorul funcționează pe baterii. Bifând această căsuță, puteți extinde durata de utilizare a bateriilor dumneavoastră.
  - Opreşte sarcina dacă se trece în modul de funcționare pe baterii.

    Specificați dacă sarcina trebuie oprită atunci când calculatorul trece în modul de funcționare pe baterii.
  - Anunță calculatorul să ruleze această sarcină.

    Specificați dacă sarcina planificată trebuie să ruleze chiar şi atunci când calculatorul funcționează în modul Sleep.

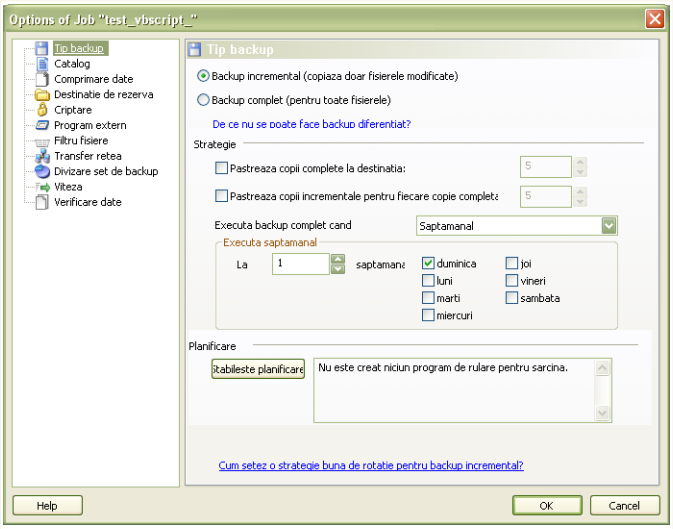
Şterge program sarcină

Pentru a şterge programul unei sarcini, selectați-o şi apoi faceți clic pe **Şterge program sarcină** în secțiunea **Gestionare sarcini**.

Dacă sarcina nu este planificată, opțiunea **Şterge program sarcină** va fi inactivă.

Modifică opțiuni sarcină

Pentru a modifica opțiunile unei sarcini, selectați-o şi apoi faceți clic pe **Modifică opțiuni sarcină** în secțiunea **Gestionare sarcini**.

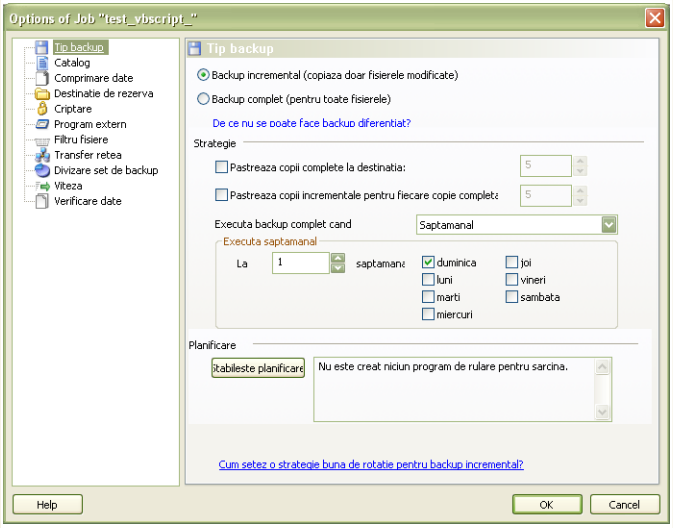


Modifică opțiuni sarcină

Sarcina selectată poate fi o sarcină de backup sau o sarcină de scriere CD/DVD. Acestea vor fi abordate pe rând în continuare.

Căsuța de dialog a opțiunilor de backup

În căsuța de dialog **Opțiuni**, există câteva sub-opțiuni.



Căsuța de dialog a opțiunilor de backup

Tip backup

Soluția de backup BitDefender suportă două tipuri de backup.

- **Backup complet:** face un backup complet al sursei selectate în setul de backup, la locația specificată. Atunci când se execută un backup complet, nu vor fi copiate doar datele modificate, ci întreaga sursă.
- **Backup incremental:** atunci când este executat prima dată, backupul incremental este identic cu backupul complet, deoarece se copiază toate datele din sursă în setul de backup la destinația specificată. După aceea însă, se face backup doar fişierelor modificate sau celor nou create. De fiecare dată când este executat un backup incremental, este creat un catalog de backup.

De asemenea, backupul incremental şi cel complet pot fi combinate într-un **Backup alternativ**. De exemplu, puteți seta un backup incremental pentru sarcină şi un backup complet o dată pe săptămână, să zicem sâmbăta. Acesta lucru se face în felul următor: selectați **Săptămânal** din meniu, 1 din câmpul **La fiecare săptămâni** şi bifați Duminică. Acest backup complet executat duminica va înlocui toate backupurile anterioare şi va reprezenta baza de la care porneşte noul backup incremental.

Catalog

Este utilizat pentru a indexa informațiile despre fişierele fiecărui backup şi reprezintă baza backupului incremental şi a procesului de restaurare. Catalogul (`*.ecs`) conține o serie de cataloage reprezentând un index al tuturor fişierelor şi directoarelor din setul de backup. Un astfel de index include informații despre momentul la care s-a făcut backupul, directorul de backup, nume şi proprietăți de fişiere. Datele pot fi restaurate din setul de cataloage.

Numele unui catalog este generat automat după destinația sarcinii. Pentru a modifica catalogul unei sarcini, urmați paşii:

1. Faceți clic pe **Catalog**.
2. Introduceți un nume de fişier în câmpul corespunzător.
3. Faceți clic pe **Caută** pentru a selecta directorul în care să fie salvate fişierele setului de cataloage.
4. Faceți clic pe **OK**.

Comprimare date

BitDefender Backup permite comprimarea şi salvarea datelor în setul de backup la executarea operației de backup pentru a salva spațiu. Acesta suportă Comprimare rapidă, Comprimare standard, Comprimare puternică. De exemplu, pentru a porni o comprimare standard la o rată şi o viteză de comprimare medie, urmați aceşti paşi:

1. Faceți clic pe **Comprimare date**.
2. Faceți clic pe **Comprimare standard**.
3. Faceți clic pe **OK**.

Destinație de rezervă

BitDefender Backup permite relocarea setului de backup către o destinație diferită. În acest caz, executarea operației de backup va continua, chiar dacă o anumită destinație nu are suficient spațiu liber.

Puteți adăuga una sau mai multe destinații pentru a continua backupul, le puteți modifica sau chiar şterge, utilizând una dintre metodele următoare:

1. Faceți clic pe **Destinație de rezervă**.
2. Faceți clic pe **Adaugă** pentru a selecta o nouă destinație pentru copia de rezervă.
3. Faceți clic pe **Editează** pentru a modifica destinația de backup selectată.
4. Faceți clic pe **Şterge** pentru a şterge destinația de backup selectată.
5. Faceți clic pe **Şterge tot** pentru a şterge toate destinațiile de backup.
6. Faceți clic pe **OK**.

Criptare

BitDefender Backup asigură o protecție adițională a datelor criptându-le înainte de a le salva la setul de backup. Setările de securitate ale unei sarcini includ şi protecția prin parolă.

Pentru a cripta datele înainte de backup, urmați aceşti paşi:
1. Faceți clic pe **Criptare**.
2. Selectați un tip de criptare din meniul drop-down.
3. Introduceți parola în câmpul corespunzător.
4. Reintroduceți parola în câmpul corespunzător.
5. Faceți clic pe **OK**.

Program extern

Sarcina poate rula altă comandă înainte sau după backup, iar comanda poate fi `.exe`, `.com` sau `.bat`, sau un anumit tip de eveniment, cum ar fi "închide calculatorul la sfârşitul backupului".

Pentru a executa comanda la pornirea backupului, urmați aceşti paşi:
1. Faceți clic pe **Program extern**.
2. Selectați opțiunea **Înainte de execuția sarcinii**.
3. Faceți clic pe **Caută** pentru a selecta fişierele de comandă care să fie executate.
4. Faceți clic pe **OK**.

Pentru a executa o comanda la sfârşitul backupului, urmați aceşti paşi:
1. Faceți clic pe **Program extern**.
2. Selectați opțiunea **După executarea sarcinii**.
3. Faceți clic pe **Caută** pentru a selecta fişierele de comandă care să fie executate.
4. Sau faceți clic pe **Oprire calculator** la sfârşitul backupului.
5. Sau faceți clic pe **Repornire calculator** la sfârşitul backupului.
6. Sau faceți clic pe **Ieşire din cont** la sfârşitul backupului.
7. Faceți clic pe **OK**.

Notă

Dacă doriți ca setările să funcționeze chiar şi în cazul unui eşec al operației de backup, bifați **Execută programul extern chiar dacă execuția sarcinii a eşuat**.

Filtru fişiere

BitDefender Backup oferă o funcție avansată de filtrare pentru a exclude sau include anumite fişiere, tipuri de fişiere sau directoare, pentru a economisi spațiul de stocare şi pentru a îmbunătăți viteza de backup.

Pot fi filtrate tipuri de fişiere urmând aceşti paşi:
1. Faceți clic pe **Filtru fişiere**.

2. Faceți clic pe **Filtrare după tip**.
3. Excludeți sau includeți tipuri de fişiere, din căsuța de dialog, bifând opțiunile **Include doar tipurile de fişiere selectate** sau **Exclude tipurile de fişiere selectate**.
4. Dacă este necesar, introduceți un alt tip de fişier în câmpul **Tip personalizat**, dar asigurați-vă că folosiți un format de tip **.** abc. Utilizați **,** (virgula) ca separator atunci când introduceți mai multe tipuri personalizate. Adăugați o scurtă descriere în câmpul corespunzător.
5. Faceți clic pe **OK**.

Pot fi filtrate fişiere urmând aceşti paşi:
1. Faceți clic pe **Filtru fişiere**.
2. Faceți clic pe **Filtrare fişiere**.
3. Excludeți sau includeți anumite fişiere, din căsuța de dialog, bifând opțiunile **Include doar fişierele desemnate de regulă** sau **Exclude fişierele desemnate de regulă**.
4. Faceți clic pe **Caută** şi selectați fişierul. Calea către locația fişierului va fi adăugată automat în câmpul **Se aplică următoarelor directoare**. Pentru a include sau exclude fişierul indiferent de locația sa, faceți clic pe **Se aplică tuturor directoarelor**.
5. Faceți clic pe **OK**.

Pot fi filtrate directoare urmând aceşti paşi:
1. Faceți clic pe **Filtru fişiere**.
2. Faceți clic pe **Filtrare directoare**.
3. Excludeți sau includeți anumite directoare, din căsuța de dialog, bifând opțiunile **Include doar directoarele desemnate de regulă** sau **Exclude directoarele desemnate de regulă**.
4. Faceți clic pe **Caută** şi selectați directorul. Calea către director va fi adăugată automat în câmpul **Se aplică următoarelor directoare**. Pentru a include sau exclude directoare indiferent de locația lor, faceți clic pe **Se aplică tuturor directoarelor**.
5. Faceți clic pe **OK**.

Filtrele pot fi modificate urmând aceşti paşi:
1. Faceți clic pe **Filtru fişiere**.
2. Faceți clic pe filtrul pe care doriți să îl modificați şi faceți clic pe **Editează**.
3. Modificați opțiunile dumneavoastră în căsuța de dialog.
4. Faceți clic pe **OK**.

Filtrele pot fi şterse urmând aceşti paşi:
1. Faceți clic pe **Filtru fişiere**.

2. Faceți clic pe filtrul pe care doriți să îl ştergeți şi apoi pe **Şterge**.
3. Sau faceți clic pe direct pe **Şterge tot** pentru a şterge toate filtrele.
4. Faceți clic pe **OK**.

Transfer rețea

BitDefender Backup permite executarea de operații de backup şi restaurare a datelor partajate din rețea. Dacă rețeaua nu este disponibilă, se va încerca executarea backupului în mod regulat. Pentru a specifica frecvența şi numărul de încercări de a face backup, urmați aceşti paşi.

1. Faceți clic pe **Transfer rețea**.
2. Faceți clic pe **Când eşuează citirea fişierelor din rețea din cauza deconectării, încearcă reconectarea la rețea**.
3. Introduceți intervalul de timp (în secunde) la care să se încerce din nou executarea operației de backup.
4. Introduceți numărul de încercări de a executa operația de backup.
5. Faceți clic pe **OK**.

Notă

Pentru a evita un surplus excesiv de informații referitoare la erori de rețea, faceți clic pe **Nu este generat niciun raport de eroare atunci când rețeaua nu este disponibilă**.

Divizare set de backup

Setul de backup generat poate fi divizat în mai multe seturi de backup, astfel încât operația de backup să poată fi executată normal chiar şi atunci când destinația sau sistemul de fişiere este limitat. BitDefender Backup oferă două metode de divizare: auto-divizarea şi divizarea bazată pe mărime.

Setările de divizare ale sarcinii pot fi modificate după cum urmează:

1. Faceți clic pe **Divide set de backup**.
2. Selectați **Divizare automată după spațiul destinației**.
3. Sau selectați **Specificați mărimea pentru divizare** şi alegeți mărimea dorită din meniu.
4. Faceți clic pe **OK**.

Viteză

BitDefender Backup suportă trei tipuri de viteză. Cu cât viteza este mai mare, cu atât va fi procesorul mai solicitat.

Viteza de backup poate fi specificată urmând aceşti paşi.

1. Faceți clic pe **Viteză**.
2. Selectați viteza **maximă**, **medie** sau **minimă**.
3. Faceți clic pe **OK**.

Verificare date

Pentru a vă asigura că datele de backup sunt întotdeauna în siguranță, urmați aceşti paşi:

1. Faceți clic pe **Verificare date**.
2. Faceți clic pe **Verifică datele în procesul de backup**.
3. Faceți clic pe **OK**.

Modifică opțiuni pentru sarcini de scriere

Mai multe opțiuni sunt disponibile în căsuța de dialog.

Scrie:

Aici puteți seta ca discul să fie ejectat după scriere, să fie finalizat (dacă doriți să îl folosiți în comun cu alte persoane) sau să fie scris utilizând sistemul de fişiere Joliet (mai puține restricții asupra numelor de fişiere).

Dacă doriți să programați sarcina, faceți clic pe **Setează program**.

Aici puteți programa sarcina de backup să ruleze la un moment convenabil. Puteți programa sarcina să fie executată zilnic, săptămânal, lunar sau la un moment dat (de exemplu, la pornirea sistemului). Programarea sarcinilor reprezintă baza backupului automat.

În cazul în care calculatorul dumneavoastră face parte dintr-un domeniu, o serie de paşi adiționali sunt necesari pentru a programa o sarcină.

1. Selectați sarcina şi apoi faceți clic pe **Planifică sarcina**.
2. Va apărea căsuța **Stabiliti utilizatorul curent**. Dacă sunteți utilizator în domeniu, introduceți parola domeniului.
3. Altfel, selectați **Acest utilizator Windows**.
4. Introduceți numele de utilizator, parola şi numele serverului de domeniu.
5. Faceți clic pe **OK**.

O dată ce ați setat utilizatorul curent, BitDefender Backup va afişa căsuța de dialog **Program** pentru a putea seta un timp convenabil pentru executarea sarcinii.

Aici puteți specifica frecvența cu care este rulată sarcina programată: zilnic, săptămânal, lunar, o singură dată, la pornirea sistemului, la logare, atunci când calculatorul nu este folosit. Dacă sarcina este planificată zilnic, săptămânal, lunar sau o singură dată, puteți specifica momentul lansării în execuție. De asemenea, puteți selecta frecvența cu care să fie rulată sarcina (exprimată prin numărul de zile sau săptămâni, ziua lunii sau data). O altă setare posibilă este durata (în minute) perioadei în care nu este utilizat calculatorul după care să fie pornită sarcina programată.

De asemenea, este posibilă configurarea mai multor programe de rulare pentru o sarcină, făcând clic pe **Afişează programe multiple**. Făcând clic pe **Avansat** puteți seta opțiuni adiționale pentru programarea sarcinii. De exemplu, puteți specifica data de început şi pe cea de sfârşit a sarcinii.

Pentru o configurare mai detaliată a programului, faceți clic pe tabul **Setări**. Sunt disponibile trei opțiuni.

- **Sarcină planificată finalizată**
  - Şterge sarcina dacă nu este programată să ruleze din nou.

    Această sarcină este utilă pentru sarcinile programate să ruleze o singură dată.
  - Opreşte sarcina dacă rulează de mai mult de:

    Specificați după cât timp de la lansarea în execuție ar trebui oprită sarcina.
- **Inactivitate**
  - Lansează sarcina în execuție doar dacă perioada de inactivitate a calculatorului este de cel puțin:

    Specificați cât timp (în minute) trebuie să treacă fără a fi utilizate mouse-ul sau tastatura pentru a lansa în execuție sarcina planificată.
  - Dacă perioada de inactivitate a calculatorului este mai mică decât cea specificată, încearcă încă:

    Specificați pentru cât timp (în minute) să fie verificată perioada de inactivitate a calculatorului.
  - Opreşte sarcina atunci când calculatorul este utilizat.

    Specificați dacă ar trebui oprită sarcina dacă începeți să utilizați calculatorul în timp ce sarcina rulează.
- **Gestionarea consumului de curent**
  - Nu lansa sarcina atunci când calculatorul funcționează pe baterii.

    Specificați dacă sarcina nu trebuie să ruleze atunci când calculatorul funcționează pe baterii. Bifând această căsuță, puteți extinde durata de utilizare a bateriilor dumneavoastră.
  - Opreşte sarcina dacă se trece în modul de funcționare pe baterii.

    Specificați dacă sarcina trebuie oprită atunci când calculatorul trece în modul de funcționare pe baterii.
  - Anunță calculatorul să ruleze această sarcină.

    Specificați dacă sarcina planificată trebuie să ruleze chiar şi atunci când calculatorul funcționează în modul Sleep.

Program extern

Sarcina poate rula altă comandă înainte sau după backup, iar comanda poate fi `.exe`, `.com` sau `.bat`, sau un anumit tip de eveniment, cum ar fi "închide calculatorul la sfârşitul backupului".

Pentru a executa comanda la pornirea backupului, urmați aceşti paşi:

1. Faceți clic pe **Program extern**.
2. Selectați opțiunea **Înainte de execuția sarcinii**.
3. Faceți clic pe **Caută** pentru a selecta fişierele de comandă care să fie executate.
4. Faceți clic pe **OK**.

Pentru a executa o comanda la sfârşitul backupului, urmați aceşti paşi:

1. Faceți clic pe **Program extern**.
2. Selectați opțiunea **După executarea sarcinii**.
3. Faceți clic pe **Caută** pentru a selecta fişierele de comandă care să fie executate.
4. Sau faceți clic pe **Oprire calculator** la sfârşitul backupului.
5. Sau faceți clic pe **Repornire calculator** la sfârşitul backupului.
6. Sau faceți clic pe **Ieşire din cont** la sfârşitul backupului.
7. Faceți clic pe **OK**.

Notă

Dacă doriți ca setările să funcționeze chiar şi în cazul unui eşec al operației de backup, bifați **Execută programul extern chiar dacă execuția sarcinii a eşuat**.

Filtru fişiere

BitDefender Backup oferă o funcție avansată de filtrare pentru a exclude sau include anumite fişiere, tipuri de fişiere sau directoare, pentru a economisi spațiul de stocare şi pentru a îmbunătăți viteza de backup.

Pot fi filtrate tipuri de fişiere urmând aceşti paşi:

1. Faceți clic pe **Filtru fişiere**.
2. Faceți clic pe **Filtrare după tip**.
3. Excludeți sau includeți tipuri de fişiere, din căsuța de dialog, bifând opțiunile **Include doar tipurile de fişiere selectate** sau **Exclude tipurile de fişiere selectate**.
4. Dacă este necesar, introduceți un alt tip de fişier în câmpul **Tip personalizat**, dar asigurați-vă că folosiți un format de tip `.abc`. Utilizați `,` (virgula) ca separator atunci când introduceți mai multe tipuri personalizate. Adăugați o scurtă descriere în câmpul corespunzător.
5. Faceți clic pe **OK**.

Pot fi filtrate fişiere urmând aceşti paşi:

1. Faceți clic pe **Filtru fişiere**.

2. Faceți clic pe **Filtrare fişiere**.
3. Excludeți sau includeți anumite fişiere, din căsuța de dialog, bifând opțiunile **Include doar fişierele desemnate de regulă** sau **Exclude fişierele desemnate de regulă**.
4. Faceți clic pe **Caută** şi selectați fişierul. Calea către locația fişierului va fi adăugată automat în câmpul **Se aplică următoarelor directoare**. Pentru a include sau exclude fişierul indiferent de locația sa, faceți clic pe **Se aplică tuturor directoarelor**.
5. Faceți clic pe **OK**.

Pot fi filtrate directoare urmând aceşti paşi:

1. Faceți clic pe **Filtru fişiere**.
2. Faceți clic pe **Filtrare directoare**.
3. Excludeți sau includeți anumite directoare, din căsuța de dialog, bifând opțiunile **Include doar directoarele desemnate de regulă** sau **Exclude directoarele desemnate de regulă**.
4. Faceți clic pe **Caută** şi selectați directorul. Calea către director va fi adăugată automat în câmpul **Se aplică următoarelor directoare**. Pentru a include sau exclude directoare indiferent de locația lor, faceți clic pe **Se aplică tuturor directoarelor**.
5. Faceți clic pe **OK**.

Filtrele pot fi modificate urmând aceşti paşi:

1. Faceți clic pe **Filtru fişiere**.
2. Faceți clic pe filtrul pe care doriți să îl modificați şi faceți clic pe **Editează**.
3. Modificați opțiunile dumneavoastră în căsuța de dialog.
4. Faceți clic pe **OK**.

Filtrele pot fi şterse urmând aceşti paşi:

1. Faceți clic pe **Filtru fişiere**.
2. Faceți clic pe filtrul pe care doriți să îl ştergeți şi apoi pe **Şterge**.
3. Sau faceți clic pe direct pe **Şterge tot** pentru a şterge toate filtrele.
4. Faceți clic pe **OK**.

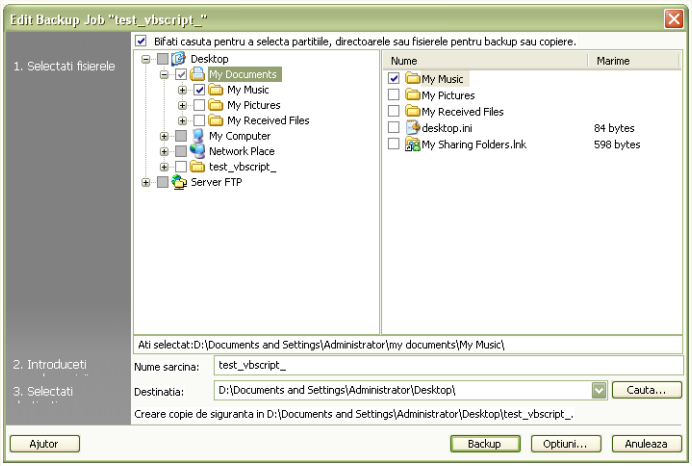
Verificare date

Pentru a vă asigura că datele de backup sunt întotdeauna în siguranță, urmați aceşti paşi:

1. Faceți clic pe **Verificare date**.
2. Faceți clic pe **Verifică datele în procesul de backup**.
3. Faceți clic pe **OK**.

Modifică proprietăți sarcină

Pentru a modifica proprietățile unei sarcini, selectați sarcina în cauză şi apoi faceți clic pe **Modifică proprietăți sarcină** în secțiunea **Manager de sarcini**.



Modifică proprietăți sarcină

1. Faceți clic pe căsuță pentru a selecta partiții, directoare şi fişiere pentru backup.

   Atunci când selectați un obiect în fereastra din partea stângă, conținutul acestuia va fi afişat în fereastra din partea dreaptă pentru a vă permite o selecție mai precisă.
2. Introduceți un nume pentru sarcina de backup sau păstrați numele implicit.

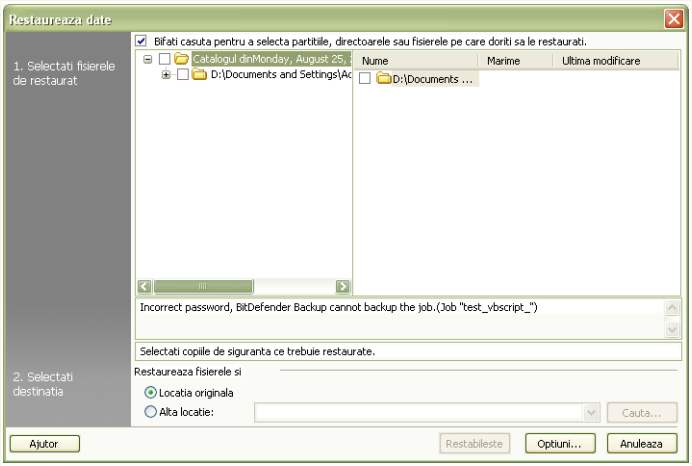
   Numele implicit al sarcinii este generat automat atunci când sunt selectate fişiere sau directoare pentru backup, dar acesta poate fi modificat.
3. Faceți clic pe **Caută** pentru a alege unde să fie salvată sarcina de backup.

Notă

Nu uitați să faceți clic pe **Backup** pentru a începe sau pe **Anulare** pentru a anula. Pentru setări detaliate, faceți clic pe **Opțiuni**.

Restaurează fişier

Pentru a restaura datele la care s-a făcut backup, selectaţi sarcina ale cărei date vreţi să fie restaurate, faceţi clic pe **Restaurează fişier** în meniul **Restaurare sarcini** şi apoi urmaţi aceşti paşi.



Restaurează fişier

1. Bifaţi căsuţele corespunzătoare partiţiilor, directoarelor sau fişierelor care doriţi a fi restaurate.

   Atunci când selectaţi un obiect în fereastra din partea stângă, conţinutul acestuia va fi afişat în fereastra din partea dreaptă pentru a vă permite o selecţie mai precisă.
2. În fereastra **Selectaţi fişierele de restaurat**, puteţi utiliza locaţia originală fără alte schimbări sau puteţi specifica o altă locaţie unde să fie restaurat fişierul.

   Faceţi clic pe **Caută** pentru a alege unde să fie salvată sarcina de backup.

Notă
Nu uitaţi să faceţi clic pe **Restaurează** pentru a începe sau pe **Anulare** pentru a anula.
Pentru setări detaliate, faceţi clic pe **Opţiuni**.

Căsuța de dialog a opțiunilor de restaurare

Opțiunile de restaurare vă permit să specificați dacă fișierele ce urmează a fi restaurate există la destinație în momentul restaurării şi dacă să fie actualizată data modificării fiecărui fișier restaurat.

Când fişierele de restaurat există deja

- **Omitere fişiere** BitDefender omite fişierele respective.
- **Întreabă utilizatorul dacă doreşte să înlocuiască fişierele** BitDefender vă consultă dacă să şteargă sau nu fişierele existente.
- **Înlocuieşte mereu fişierele automat** BitDefender înlocuieşte fişierele fără a vă avertiza.
- **Înlocuieşte doar fişierele mai vechi decât fişierul de backup** BitDefender înlocuieşte doar fişierele mai vechi. Acestea sunt determinate pe baza datei la care au fost modificate ultima oară.

Data modificării fişierului

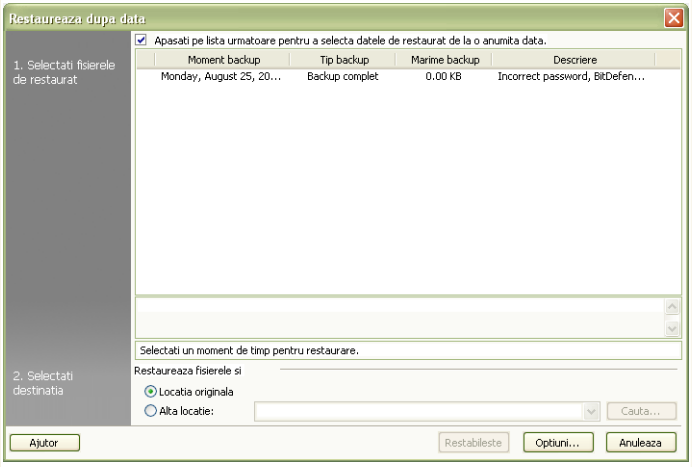
Dacă opțiunea este selectată, BitDefender utilizează data curentă pentru a indica data la care au fost restaurate fişierele şi directoarele. Altfel, BitDefender utilizează ca dată de modificare a fişierelor şi directoarelor data la care acestora li s-au făcut copii de siguranță.

Structură directoare

Devine activă doar atunci când alegeți o altă locație la care să fie restaurate datele. De asemenea, puteți păstra structura curentă a directoarelor.

Restaurează după dată

Pentru a restaura date la care ați făcut copii de siguranță la un anumit moment, selectați sarcina ale cărei date să fie restaurate, faceți clic pe **Restaurează după dată** în meniul **Restaurare sarcini** şi urmați aceşti paşi.



Restaurează după dată

1. Selectați din listă setul de backup de la un anumit moment de timp. Sub acesta vor fi afişate observațiile corespunzătoare.
2. În fereastra **Selectare locație restaurare**, puteți utiliza locația originală, fără alte modificări, sau puteți specifica o altă locație la care să fie restaurat fişierul.

   Faceți clic pe **Caută** pentru a alege unde să fie salvată sarcina de backup.

Notă

Nu uitați să faceți clic pe **Restaurează** pentru a începe sau pe **Anulare** pentru a anula.
Pentru setări detaliate, faceți clic pe **Opțiuni**.

Căsuța de dialog a opțiunilor de restaurare

Opțiunile de restaurare vă permit să specificați dacă fişierele ce urmează a fi restaurate există la destinație în momentul restaurării şi dacă să fie actualizată data modificării fiecărui fişier restaurat.

Când fişierele de restaurat există deja

- **Înlocuieşte doar fişierele mai vechi decât fişierul de backup** BitDefender înlocuieşte doar fişierele mai vechi. Acestea sunt determinate pe baza datei la care au fost modificate ultima oară.

Data modificării fişierului

Dacă opțiunea este selectată, BitDefender utilizează data curentă pentru a indica data la care au fost restaurate fişierele şi directoarele. Altfel, BitDefender utilizează ca dată de modificare a fişierelor şi directoarelor data la care acestora li s-au făcut copii de siguranță.

Structură directoare

Devine activă doar atunci când alegeți o altă locație la care să fie restaurate datele. De asemenea, puteți păstra structura curentă a directoarelor.

Control sarcini

O sarcină poate fi controlată în trei moduri: întrerupere sarcină, oprire sarcină şi oprire toate.

Întrerupe

Pentru a întrerupe o sarcină de backup sau de restaurare, faceți clic pe butonul **Întrerupe sarcină** din meniul **Control sarcini**.

Opreşte

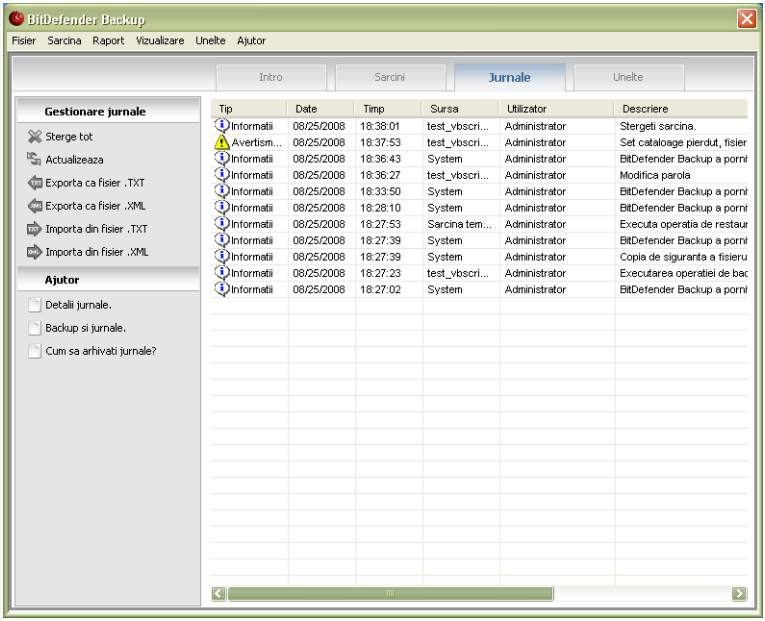
Pentru a opri o sarcină activă de backup sau de restaurare, faceți clic pe butonul **Opreşte sarcină** din meniul **Control sarcini**.

Opreşte tot

Dacă rulează mai multe sarcini de backup sau restaurare, nu este nevoie să le opriți una câte una. Faceți clic pe butonul **Opreşte tot** din meniul **Control sarcini** pentru a le opri pe toate imediat.

Jurnale

Această secțiune vă arată cum să vizualizați, să importați, să exportați şi să ştergeți jurnale. Opțiunea Jurnale vă ajută să rețineți ce ați salvat sau restaurat şi când, şi, de asemenea, afişează avertismentele şi erorile apărute în timpul efectuării acestor operații. De exemplu, dacă a apărut o eroare la citirea unui fişier în timpul execuției, aceasta a fost înregistrată de BitDefender ca avertisment.



Jurnale

Puteți comuta pe fereastra **Jurnale** folosind una dintre următoarele metode:

- Faceți clic pe **Jurnale** în **bara de navigare**.
- Faceți clic pe **Vizualizare** în **bara de meniuri** şi selectați **Jurnale**.
- Utilizați o scurtătură apăsând **CTRL+Alt+L**.

Vizualizare jurnale

Opțiunea de vizualizare a jurnalelor permite verificarea executării operației şi depistarea motivului care a dus la eşecul acesteia.

Descrierea unui obiect din jurnalul BitDefender Backup conține următoarele evenimente:

Tip

O clasificare a severității obiectului din jurnal. Există patru niveluri de severitate:

- **Fatal:** o problemă importantă care împiedică funcționarea normală a BitDefender Backup. De exemplu, atunci când a fost corupt fişierul de configurare a BitDefender Backup.
- **Eroare:** o problemă care duce la eşuarea unei operații. De exemplu, se încearcă executarea unei operații de backup la o sarcină pe un server, dar serverul nu poate fi accesat.
- **Avertisment:** o problemă care nu afectează o operație, dar care poate fi clasificată mai târziu ca eveniment. De exemplu, un fişier care nu poate fi citit atunci când i se face o copie de rezervă.
- **Informații:** Descrie o operație realizată cu succes. De exemplu, o sarcină ştearsă cu succes.

Dată
Data la care a apărut obiectul în jurnal.

Timp
Momentul la care s-a produs evenimentul înregistrat.

Sursă
Sursa care a înregistrat evenimentul respectiv, care poate fi o sarcină sau aplicația BitDefender Backup. De exemplu, un eveniment marcat Sistem indică faptul că a fost înregistrat de către BitDefender Backup. Alte marcaje posibile sunt numele sarcinilor care au înregistrat evenimentul respectiv.

Utilizator
Numele utilizatorului pe baza acțiunii căruia a fost înregistrat evenimentul.

Descriere
Prezintă amănunțit conținutul evenimentului înregistrat.

Şterge jurnale

BitDefender Backup oferă două metode de a şterge jurnale: automat şi manual.

Important
O dată ştearsă, o înregistrare nu mai poate fi recuperată. De aceea, este recomandat să exportați toate jurnalele şi să le salvați pentru a le putea consulta ulterior.

Ştergere automată
La pornire, BitDefender Backup compară mărimea jurnalului existent cu mărimea standard a jurnalului. Toate fişierele de jurnal ce depăşesc mărimea standard sunt şterse automat de către BitDefender Backup.

Notă
Pentru a afla sau modifica mărimea implicită a fişierului de raport, urmaţi aceşti paşi:
1. Faceţi clic pe **Unelte** în **bara de meniuri**.
2. Faceţi clic pe **Opţiuni** şi apoi selectaţi **Rapoarte & Jurnal**.
3. Introduceţi mărimea limită dorită (în MB) în câmpul corespunzător. Atunci când mărimea jurnalului atinge această limită, BitDefender Backup va şterge toate jurnalele.

Ştergere manuală

Urmaţi aceşti paşi pentru a şterge jurnalele manual.
1. Faceţi clic pe **Şterge tot** în meniul **Gestionare jurnal**.
2. Faceţi clic pe **OK** pentru a exporta anumite jurnale înainte de ştergerea celorlalte, sau faceţi clic pe **Nu** dacă nu doriţi să salvaţi niciun jurnal.

Importare şi exportare de jurnale

Soluţia de backup BitDefender suportă în mod curent import şi export de fişiere în două formate: `.TXT` şi `.XML`

Notă
Vă recomandăm să exportaţi şi să salvaţi jurnalul înainte de a-l şterge.

Pentru a exporta jurnalele într-un fişier specificat, urmaţi aceşti paşi:

1. Faceţi clic pe **Exportă ca fişier .TXT** sau **Exportă ca fişier .TXT** în meniul **Gestionare jurnale**.
2. Introduceţi numele fişierului şi selectaţi o locaţie unde acesta să fie salvat.
3. Faceţi clic pe **Salvează**.

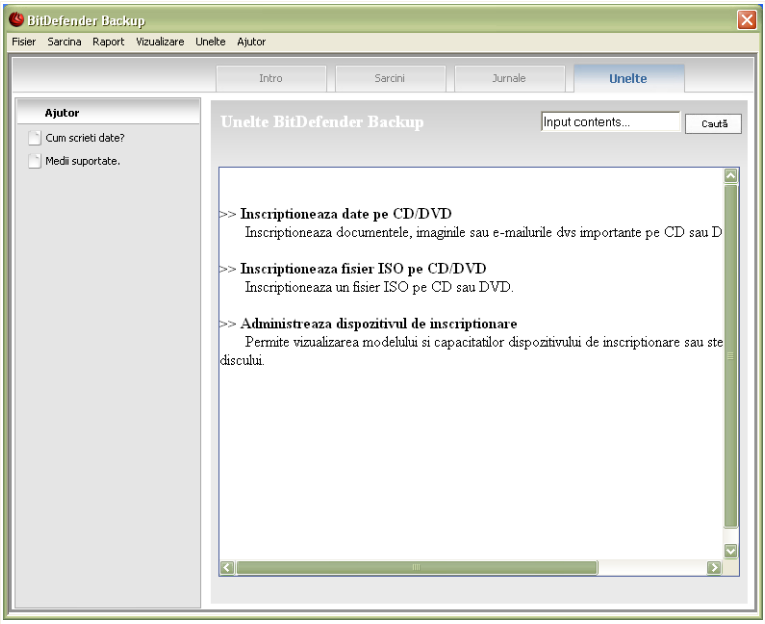
Pentru a importa jurnale dintr-un anumit fişier, urmaţi aceşti paşi:

1. Faceţi clic pe **Importă din fişier .TXT** sau pe **Importă din fişier .TXT** în meniul **Gestionare jurnale**.
2. Localizaţi fişierul.
3. Faceţi clic pe **Deschide**.

Notă
Faceţi clic pe butonul **Actualizează** din meniul **Gestionare jurnale** pentru a vă asigura că vedeţi ultimele jurnale.

Unelte

Această secțiune vă arată cum să folosiți BitDefender Backup pentru a scrie date pe CD/DVD sau pentru a scrie un fişier imagine ISO. Sunt tratate subiecte precum scrierea unui CD-R/RW, DVD-R/RW/RAM, DVD+R/RW/DL şi păstrarea copiilor de siguranță offline.



Unelte

Puteți comuta pe fereastra **Unelte** folosind una dintre următoarele metode:

- Faceți clic pe **Unelte** în **bara de navigare**.
- Faceți clic pe **Vizualizare** în **bara de meniuri** şi selectați **Unelte**.
- Utilizați o scurtătură apăsând **CTRL+Alt+T**.

Scrie pe CD/DVD

Pentru a scrie date manual pe un CD/DVD, urmați aceşti paşi:

1. Faceți clic pe **Scrie date pe CD/DVD**
2. Faceți clic pe **Şterge** dacă doriți să reutilizați un disc reutilizabil. Dacă doriți să îl ştergeți rapid, faceți clic pe **Rapid**. Dacă doriți ca acesta să fie şters complet, faceți clic pe **Complet**, procesul necesitând un timp mai îndelungat.
3. Faceți clic pe **Scrie cu mesaje**.

   Aici puteți seta ca discul să fie ejectat după scriere, să fie finalizat (dacă doriți să îl folosiți în comun cu alte persoane) sau să fie scris utilizând sistemul de fişiere Joliet (mai puține restricții asupra numelor de fişiere).
4. Faceți clic pe **Fişier** sau **Director** în fereastra de dialog pentru a adăuga datele care doriți să fie scrise.
5. După adăugarea datelor, selectați utilitarul de scriere şi numele discului pe care scrieți datele, şi apoi faceți clic pe **Scrie**.

Scrie fişiere imagine ISO pe CD/DVD:

Pentru a scrie un fişier imagine ISO pe un CD/DVD, urmați aceşti paşi:

1. Faceți clic pe **Scrie fişiere ISO pe CD/DVD**
2. Faceți clic pe **Şterge** dacă doriți să reutilizați un disc reutilizabil. Dacă doriți să îl ştergeți rapid, faceți clic pe **Rapid**. Dacă doriți ca acesta să fie şters complet, faceți clic pe **Complet**, procesul necesitând un timp mai îndelungat.
3. Faceți clic pe **Scrie cu mesaje**.

   Aici puteți seta ejectarea discului după scriere, finalizarea discului (dacă doriți să îl utilizați în comun cu alte persoane) sau scrierea datelor utilizând sistemul de fişiere Joliet (mai puține restricții asupra numelor de fişiere).
4. Faceți clic pe **Adaugă**.
5. Selectați un fişier imagine ISO care să fie scris şi faceți clic pe **Deschide**.
6. Faceți clic pe **Scrie**.

Administrare utilitar de scriere

Vă ajută să gestionați şi să vizualizați mediul şi dispozitivul de stocare de pe sistemul curent. Conține următoarele linkuri:

- **Ejectează dispozitiv** Ejectează suportul de memorare selectat.
- **Închide dispozitiv** Închide dispozitivul de memorare selectat.
- **Informații mediu** permite vizualizarea informațiilor despre mediul dispozitivului de memorare.
- **Informații dispozitiv** Permite vizualizarea informațiilor dispozitivului de memorare.
- **Posibilități** Permite vizualizarea posibilităților mediului de memorare.
- **Şterge mediu** Şterge conținutul discului.

21. Criptare

BitDefender oferă capabilități de criptare pentru a vă proteja documentele confidențiale şi conversațiile dumneavoastră prin mesageria instant, prin Yahoo Messenger şi MSN Messenger.

21.1. 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 foloseste o aplicație web pentru chat, cum ar fi Meebo, sau alte aplicații de chat care suportă Yahoo Messenger sau MSN.

Pentru a configura criptarea mesageriei instant, mergeți la **Criptare>Criptare IM** în modul avansat.

Notă
Puteți configura uşor criptarea mesageriei instant folosind bara de comenzi BitDefender din fereastra de chat. Pentru mai multe informații, consultați "*Integrarea cu clienții de mesagerie instant*" (p. 52).

Criptare mesagerie instant

Implicit, criptarea mesageriei instant este activată atât pentru Yahoo Messenger, cât şi pentru Windows Live (MSN) Messenger. Puteți alege să dezactivați complet criptarea mesageriei instant sau doar pentru o anumită aplicație de chat.

Sunt afişate două tabele:

- **Excluderi criptare** - afişează id-urile de utilizator şi programul de mesagerie instant (IM) asociat pentru care criptarea este dezactivată. Pentru a şterge un contact din listă, selectați-l şi faceți clic pe butonul **Şterge**.
- **Conexiuni curente** - afişează conexiunile de mesagerie instant curente (ID utilizator şi program IM asociat) şi 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.

21.1.1. Dezactivarea criptării pentru anumiți utilizatori

Pentru a dezactiva criptarea pentru un anumit utilizator, urmați aceşti paşi:

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**.

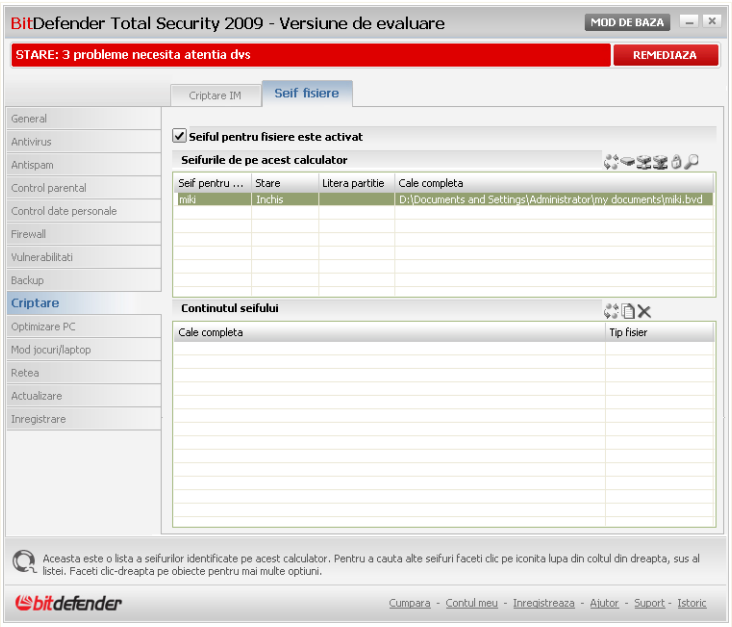
21.2. Seif de fişiere

Seiful de fişiere BitDefender vă permite să creați pe calculatorul dumneavoastră partiții logice (seifuri) criptate şi 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 şi să îl închideți pentru a-i proteja conținutul. Cât timp seiful este deschis, puteți adăuga fişiere noi şi puteți accesa sau modifica fişierele existente.

La nivel fizic, seiful este de fapt un fişier criptat de pe hard discul dumneavoastră, având extensia `bvd`. Deşi fişierele 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 fişiere de pe calculatorul dumneavoastră, mergeţi la **Criptare>Seif fişiere** în modul avansat.



Seif de fişiere

Pentru a dezactiva seiful de fişiere, debifaţi căsuţa **Seiful de fişiere este activat** şi faceţi clic pe **Da** pentru confirmare. Dacă dezactivaţi Seiful de fişiere, toate seifurile de fişiere vor fi închise şi nu veţi mai putea accesa fişierele pe care acestea le conţin.

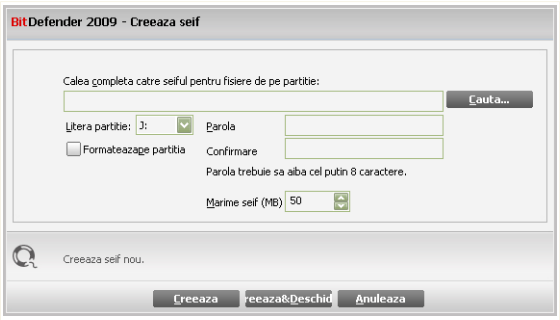
Tabelul din partea de sus afişează seifurile de fişiere de pe calculatorul dumneavoastră. Puteţi vedea numele seifului, starea acestuia (deschis / închis), litera partiţiei corespunzătoare şi calea completă către acesta. Tabelul din partea de jos afişează conţinutul seifului selectat.

21.2.1. Crearea unui seif

Pentru a crea un seif, utilizaţi una dintre aceste metode:

- Faceți clic pe **Creează seif**.
- Faceți clic-dreapta în tabelul cu seifuri şi selectați **Creează**.
- Faceți clic-dreapta pe desktop sau într-un director de pe calculatorul dumneavoastră, duceți cursorul deasupra opțiunii **Seif BitDefender** şi selectați **Creează**.

Va apărea o nouă fereastră.



Creare seif de fişiere

Procedați astfel:

1. Specificați locația şi numele seifului de fişiere.
   - Faceți clic pe **Caută**, selectați locația seifului şi salvați fişierul seif cu numele dorit.
   - Introduceți calea completă pe disc a fişierului seif.
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 parola seifului în câmpul **Parolă**. Oricine va încerca să deschidă seiful şi să acceseze fişierele acestuia va trebui să furnizeze parola.
4. Selectați **Formatează partiția** pentru a formata partiția virtuală corespunzătoare seifului.
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 şi a afişa seiful ca partiție virtuală în My Computer, faceți clic pe **Creează&Deschide**.

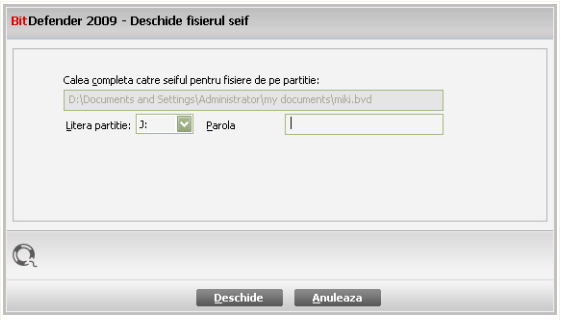
21.2.2. Deschiderea unui seif

Pentru a accesa şi a lucra cu fişierele 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 şi faceți clic pe **Deschide seif**.
- Faceți clic-dreapta pe seif în tabel şi selectați **Deschide**.
- Faceți clic-dreapta pe fişierul seif de pe calculatorul dumneavoastră, duceți cursorul deasupra opțiunii **Seif BitDefender** şi selectați **Deschide**.

Va apărea o nouă fereastră.



Deschide seif de fişiere

Procedați astfel:

1. Selectați din meniu o literă pentru partiție.
2. Introduceți parola seifului în câmpul **Parolă**.
3. Faceți clic pe **Deschide**.

21.2.3. Închiderea unui seif

Atunci când ați terminat de lucrat într-un seif de fişiere, trebuie să îl închideți pentru a vă proteja datele.

Pentru a închide un seif, utilizați una dintre aceste metode:

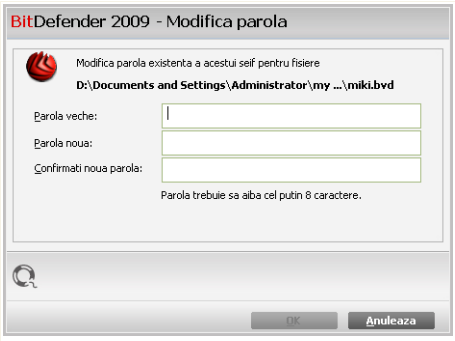
- Selectați seiful din tabel şi faceți clic pe **Închide seif**.
- Faceți clic-dreapta pe seif în tabel şi selectați **Închide**.
- Faceți clic-dreapta pe fişierul seif de pe calculatorul dumneavoastră, duceți cursorul deasupra opțiunii **Seif BitDefender** şi selectați **Închide**.
- Faceți clic-dreapta pe partiția virtuală corespunzătoare din My Computer, duceți cursorul deasupra opțiunii **Seif BitDefender** şi selectați **Închide**.

21.2.4. Modificarea parolei seifului

Pentru a modifica parola unui seif, utilizați una dintre aceste metode:

- Selectați seiful din tabel şi faceți clic pe **Modifică parola**.
- Faceți clic-dreapta pe seif în tabel şi selectați **Modifică parola**.
- Faceți clic-dreapta pe fişierul seif de pe calculatorul dumneavoastră, duceți cursorul deasupra opțiunii **Seif BitDefender** şi 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** şi **Confirmă noua parolă**.

   Notă
   Parola trebuie să conțină minim 8 caractere. Pentru a crea o parolă puternică, utilizați o combinație de litere mari şi mici, numere şi caractere speciale (cum ar fi #, $ sau @).

3. Faceți clic pe **OK** pentru a schimba parola.

21.2.5. Adăugarea fișierelor într-un seif

Pentru a adăuga fişiere într-un seif, urmați aceşti paşi:

1. Faceți clic pe **Adaugă fişier**. Va apărea o nouă fereastră.
2. Selectați fişierele / directoarele pe care doriți să le adăugați în seif.
3. Faceți clic pe **OK** pentru a copia obiectele selectate în seif.

Notă
Nu puteți adăuga în seif fişiere de sistem sau aplicații.

21.2.6. Ştergerea fișierelor dintr-un seif

Pentru a şterge fişiere dintr-un seif, urmați aceşti paşi:

1. Selectați din tabelul cu seifuri seiful care conține fişierul pe care doriți să-l ştergeți.
2. Selectați fişierul pe care doriți să-l ştergeți din tabelul care afişează conținutul seifului.
3. Faceți clic pe **Şterge fişier**.

Notă
Dacă seiful este deschis, puteți şterge direct fişierele de pe partiția logică virtuală corespunzătoare seifului.

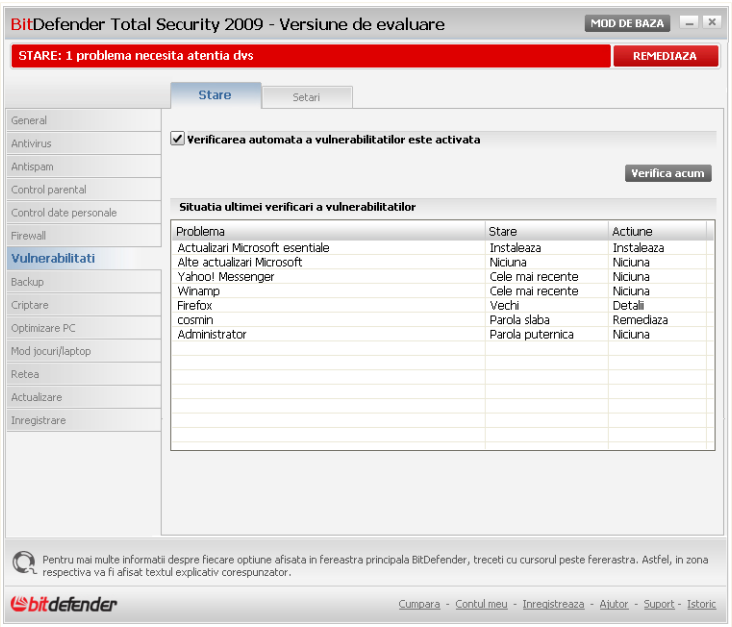
22. Vulnerabilitate

Un pas important în protejarea calculatorului dumneavoastră împotriva persoanelor răuvoitoare şi a aplicațiilor malițioase este de a menține actualizat sistemul de operare şi 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 uşurință) pentru fiecare cont de utilizator Windows.

BitDefender verifică în mod regulat sistemul dumneavoastră în căutare de vulnerabilități şi vă informează despre problemele existente.

22.1. Stare

Pentru a configura verificarea automată a vulnerabilităților sau pentru a verifica vulnerabilitățile sistemului, mergeți la **Vulnerabilitate>Status** în modul avansat.



Stare vulnerabilități

Important
Pentru a fi informat automat despre vulnerabilitățile sistemului sau aplicațiilor dumneavoastră, mențineți **Verificarea automată a vulnerabilităților** activată.

22.1.1. Căutare după vulnerabilități

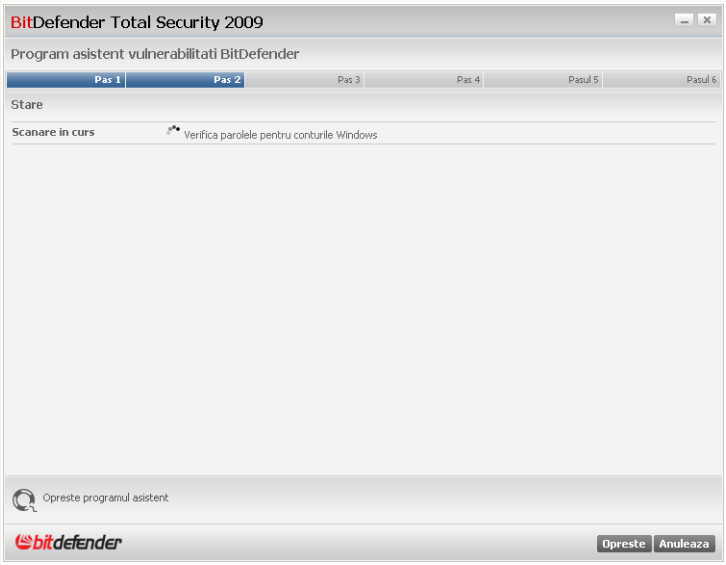
Pentru a verifica dacă sistemul dumneavoastră este vulnerabil, faceți clic pe **Verifică acum** şi urmați paşii programului asistent.

Pasul 1/6 - Selectați vulnerabilitățile de verificat

Vulnerabilități

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

Pasul 2/6 - Căutare vulnerabilități



Căutare vulnerabilități

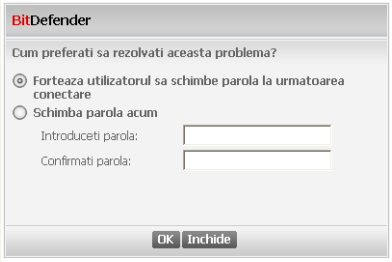
Aşteptați ca BitDefender să finalizeze căutarea.

Pasul 3/6 - Schimbați parolele slabe

Parole utilizatori

Puteti vedea lista conturilor de utilizator Windows configurate pe calculatorul dumneavoastră şi de nivelul de protecție asigurat de parola acestora.

Faceți clic pe **Repară** 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.

Notă
Pentru a crea o parolă puternică, utilizați o combinație de litere mari şi mici, numere şi caractere speciale (cum ar fi #, $ sau @).

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

Faceți clic pe **Înainte**.

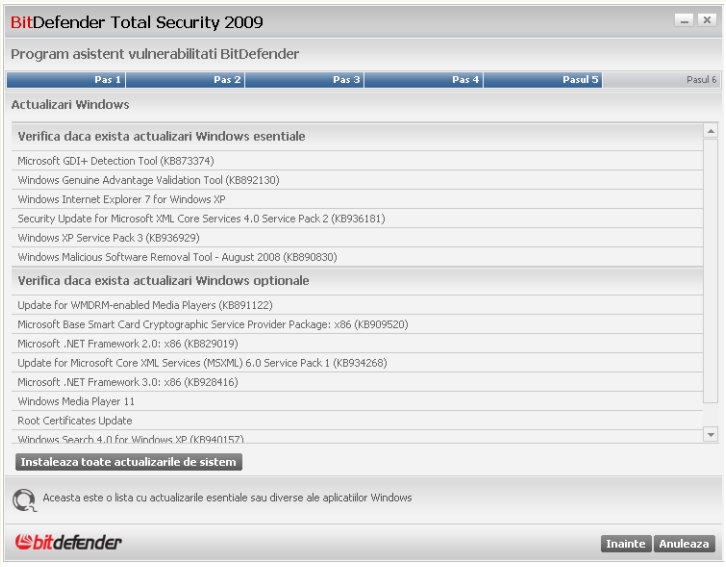
Pasul 4/6 - Actualizați aplicații

Aplicații

Puteți vedea lista aplicațiilor verificate de BitDefender şi 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**.

Pasul 5/6 - Actualizați Windows



Actualizări Windows

Puteți vedea lista actualizărilor critice şi 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**.

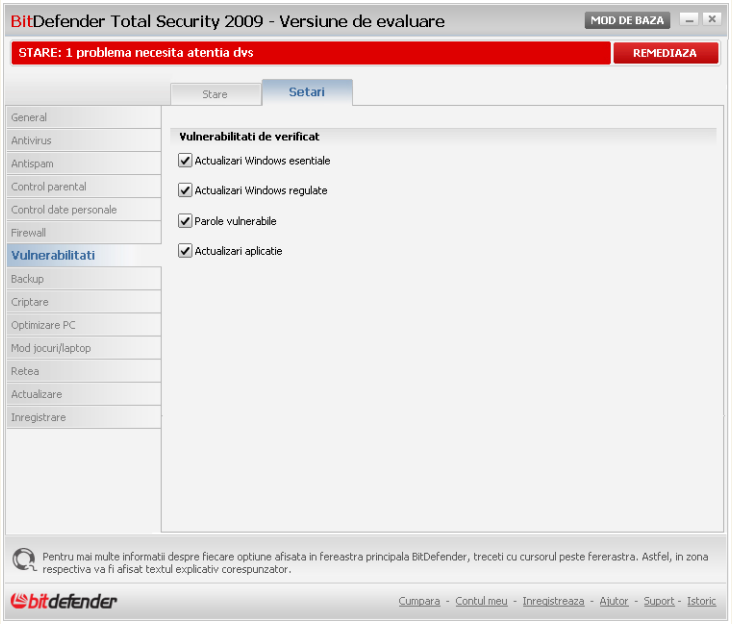
Pasul 6/6 - Examinați rezultatele

Rezultate

Faceți clic pe **Închide**.

22.2. Setări

Pentru a configura setările verificării automate a vulnerabilităților, mergeți la **Vulnerabilitate>Setări** în modul avansat.



Setări pentru verificarea automată a vulnerabilităților

Selectați căsuțele corespunzătoare vulnerabilităților care să fie verificate în mod regulat.

- **Actualizări Windows critice**
- **Actualizări Windows obişnuite**
- **Parole slabe**
- **Actualizări aplicații**

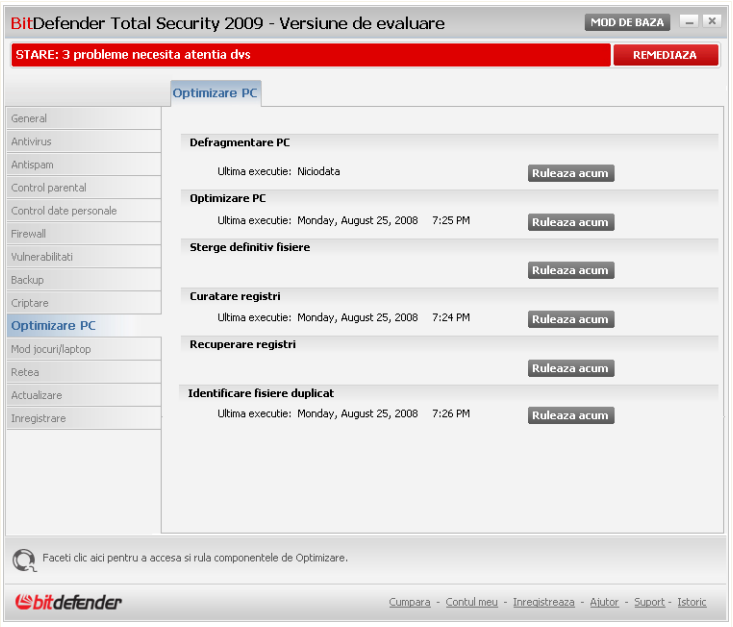
Notă

Dacă debifați căsuța corespunzătoare unei anumite vulnerabilități, BitDefender nu vă va mai avertiza despre problemele asociate.

23. Optimizare PC

BitDefender conține un modul de Optimizare PC care vă ajută să păstrați integritatea sistemului dumneavoastră. Utilitarele oferite sunt critice pentru îmbunătățirea performanței sistemului dumneavoastră şi gestionarea eficientă a spațiului pe hard disc.

Pentru a executa operații de mentenanță asupra calculatorului dumneavoastră, mergeți la **Optimizare PC** şi utilizați funcțiile oferite.



Optimizare PC

BitDefender oferă următoarele funcții de optimizare a calculatorului:

- Defragmentare PC reorganizează datele de pe hard-disc la nivel fizic astfel încât bucățile ce compun fiecare fişier să fie stocate cât mai aproape unele de altele şi în mod continuu.

- Curățare PC şterge fişierele temporare de pe Internet şi fişierele cookie, fişierele de sistem neutilizate şi scurtăturile către documentele utilizate recent.
- Distrugere fişiere şterge permanent fişiere şi urmele acestora de pe sistemul dumneavoastră. Utilizați funcția Distrugere fişiere pentru a vă asigura că fişierele pe care le ştergeți de pe calculatorul dumneavoastră nu pot fi deloc recuperate.
- Curățare regiştri identifică şi şterge referințele nevalide sau orfane din regiştrii Windows. Pentru a menține regiştrii Windows curați şi optimizați, este recomandat să executați lunar o curățare a regiştrilor.
- Recuperare regiştri poate recupera cheile de regiştri din regiştrii Windows şterse anterior utilizând funcția Curățare regiştri a BitDefender.
- Căutare duplicate descoperă şi şterge fişierele duplicat de pe sistemul dumneavoastră.

Pentru a utiliza una dintre aceste funcții, faceți clic pe **Execută acum** şi urmați paşii programului asistent.

23.1. Defragmentarea volumelor hard-discului

La copierea unui fişier ce depăşeşte mărimea celui mai mare bloc de spațiu liber pe hard-disc se produce fragmentarea fişierului. Deoarece nu este îndeajuns spațiu liber continuu pentru a stoca întregul fişier, acesta va fi stocat în mai multe blocuri. Atunci când fişierul fragmentat este accesat, informația conținută de acesta este citită din mai multe locații diferite.

Fragmentarea fişierelor încetineşte accesul la fişiere şi scade performanța sistemului. De asemenea, aceasta accelerează uzura hard-discului.

Pentru a diminua gradul de fragmentare al fişierelor trebuie să defragmentați hard-discul periodic. Prin defragmentare, informațiile de pe hard-disc sunt reorganizate la nivel fizic astfel încât bucățile ce compun fiecare fişier să fie stocate cât mai aproape şi în mod continuu. De asemenea, prin defragmentare, se încearcă crearea unor porțiuni cât mai mari de spațiu liber, pentru a preveni fragmentarea ulterioară a fişierelor.

Defragmentarea hard-discului este recomandată pentru:

- accesarea mai rapidă a fişierelor.
- îmbunătățirea performanței globale a sistemului.
- extinderea duratei de viață a hard-discului.

Pentru a defragmenta hard-discul, urmați aceşti paşi:

1. În modul avansat, faceți clic pe **Optimizare PC** în meniul din stânga.
2. Faceți clic pe butonul **Execută acum** corespunzător funcției Defragmentare PC.
3. Urmați programul asistent în trei paşi.

Notă
Defragmentarea poate dura destul de mult deoarece implică mutarea unor blocuri de date dintr-un loc în altul pe hard disc. Este recomandat să inițiați defragmentarea atunci când nu utilizați calculatorul.

23.1.1. Step 1/3 - Analizare...

Programul asistent de defragmentare va analiza hard discul pentru a stabili dacă trebuie defragmentat sau nu.

Analizare

Aşteptați ca analiza să fie finalizată. Dacă doriți să anulați această operație, faceți clic pe **Anulare**.

23.1.2. Pasul 2/3 - Examinați raportul de analiză

După finalizarea analizei, va apărea o nouă fereastră, unde puteți vedea rezultatele analizei şi puteți iniția defragmentarea hard discului, dacă aceasta este necesară.

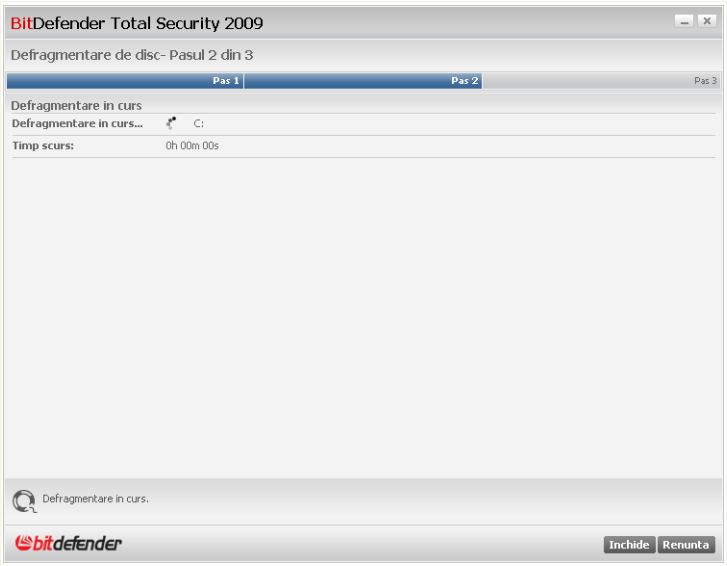
Raportul de analiză

Verificați raportul de analiză.

Dacă nicio partiție nu necesită defragmentare, faceți clic pe **Închide** pentru a închide fereastra. Altfel, selectați opțiunea **Defragmentează** corespunzătoare partițiilor care necesită defragmentare şi faceți clic pe **Execută** pentru a iniția defragmentarea.

Notă

Pentru a putea defragmenta un volum este necesar ca un procent de 15% din acesta să fie spațiu liber. Dacă nu este îndeajuns spațiu liber pe volumul ce trebuie defragmentat, atunci defragmentarea va fi abandonată.



Defragmentare

Aşteptați ca defragmentarea hard discului să fie finalizată. Puteți anula defragmentarea în orice moment făcând clic pe **Închide**.

23.1.3. Pasul 3/3 - Examinați raportul defragmentării

După ce defragmentarea hard discului a fost finalizată, va apărea o nouă fereastră, unde puteți vedea statisticile defragmentării.

Raportul defragmentării

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

23.2. Curățarea calculatorului personal

De fiecare dată când vizitați o pagină web, sunt create fişiere Internet temporare pentru a permite accesul mai rapid la pagina respectivă data viitoare când o vizitați. Cu toate că sunt denumite temporare, aceste fişiere nu sunt şterse după ce închideți browserul. Aceasta poate reprezenta o amenințare la adresa intimității dumneavostră, deoarece aceste fişiere pot fi examinate de oricine are acces la calculatorul dumneavoastră. În plus, cu trecerea timpului, aceste fişiere vor ocupa din ce în ce mai mult spațiu pe hard disc.

De asemenea, atunci când vizitați o pagină web, pe calculatorul dumneavostră sunt stocate fişiere cookie. Fişierele cookie sunt fişiere de mici dimensiuni ce conțin informații referitoare la preferințele dumneavostră legate de navigarea pe Internet. Acestea pot fi o amenințare la adresa intimității dumneavoastră, deoarece pot fi

analizate şi folosite de specialişti în publicitate pentru a vă urmări interesele şi gusturile privitoare la Internet.

Curățare PC vă ajută să eliberați spațiu pe disc şi să vă protejați confidențialitatea ştergând fişiere care nu mai sunt utile.

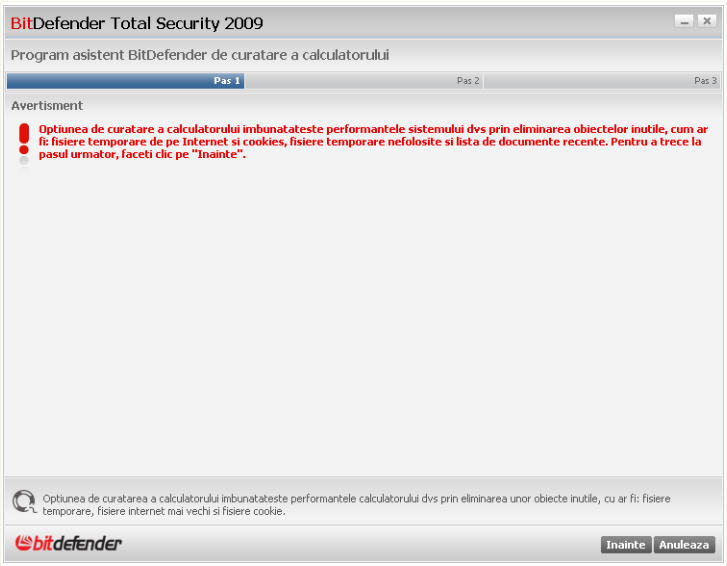
- fişierele Internet temporare şi fişierele cookie ale Internet Explorer.
- fişierele Internet temporare şi fişierele cookie ale Mozilla Firefox.
- fişierele temporare de sistem create de Windows în timpul funcționării.
- scurtăturile către documentele utilizate recent create de Windows atunci când deschideți un fişier.

Pentru a curăța sistemul de fişiere Internet temporare şi fişiere cookie, de fişierele de sistem temporare şi de scurtăturile către documentele utilizate recent, urmați aceşti paşi:

1. În modul avansat, faceți clic pe **Optimizare PC** în meniul din stânga.
2. Faceți clic pe butonul **Execută acum** corespunzător funcției Curățare PC.
3. Urmați programul asistent în trei paşi.

23.2.1. Pasul 1/3 - Inițiați ştergerea

Aici puteți inița ştergerea fişierelor Internet temporare şi a fişierelor cookie.



Fereastra de întâmpinare

Faceți clic pe **Înainte**.

23.2.2. Pasul 2/3 - Ștergere fișiere...

Programul asistent va începe ştergerea fişierelor Internet temporare şi a fişierelor cookie.

Ştergere fişiere...

Aşteptaţi ca fişierele Internet temporare şi fişierele cookie să fie şterse. Dacă doriţi să anulaţi această operaţie, faceţi clic pe **Anulare**.

23.2.3. Pasul 3/3 - Examinaţi rezultatele

După ce toate fişierele au fost şterse, va apărea o nouă fereastră, unde puteţi vedea rezultatele.

Rezultate

Puteți vedea statisticile referitoare la fişierele şterse.

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

23.3. Ştergerea permanentă a fişierelor

Atunci când ştergeți un fişier, acesta nu mai poate fi accesat prin mijloace normale. Cu toate acestea, fişierul continuă să existe pe hard disc până ce este suprascris prin copierea altor fişiere.

Chiar dacă ştergeți un fişier, acesta poate fi recuperat utilizând programe specializate. Ca urmare, apare o posibilă amenințare la adresa datelor dumneavostră personale, deoarece pot exista încercări ale unor persoane răuvoitoare de a recupera aceste date.

Pentru a elimina posibilitatea ca datele cu caracter personal şterse să poată fi recuperate, puteți utiliza BitDefender pentru a şterge la nivel fizic datele respective de pe hard discul dumneavoastră.

Pentru a şterge fişiere permanent, urmați aceşti paşi:

1. În modul avansat, faceți clic pe **Optimizare PC** în meniul din stânga.
2. Faceți clic pe butonul **Execută acum** corespunzător funcției Distrugere fişiere.
3. Urmați programul asistent în trei paşi.

23.3.1. Pasul 1/3 - Selectați locația

Aici puteți specifica ce fişiere şi directoare să fie şterse definitiv.

Țintă

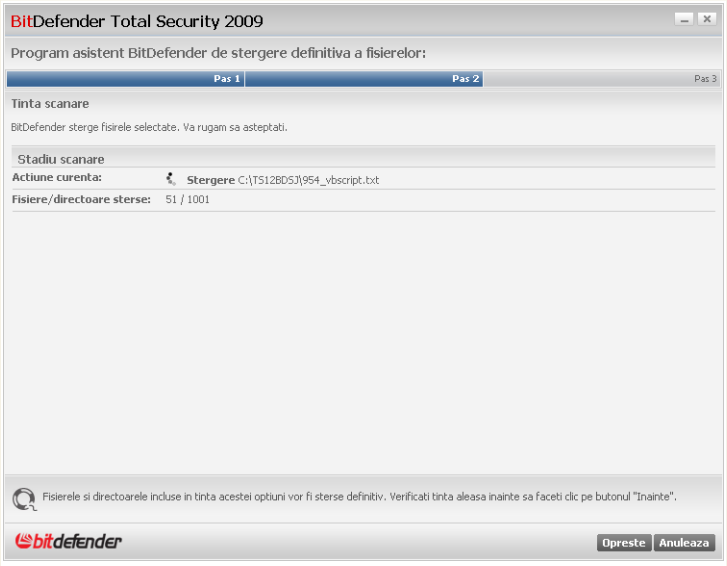
Faceți clic pe **Adaugă locație**, selectați fişierul sau directorul care doriți să fie şters şi faceți clic pe **OK**. Calea către locația selectată va apărea în coloana **Cale**. Dacă vă răzgândiți în legătură cu locația, faceți clic pe butonul **Şterge** de lângă aceasta.

Notă
Puteți selecta una sau mai multe locații.

Faceți clic pe **Înainte**.

23.3.2. Pasul 2/3 - Ștergere fișiere...

BitDefender va şterge definitiv fişierele din locațiile specificate.



Ștergere...

Aşteptați finalizarea operației de ştergere ireversibilă a fişierelor. Dacă doriți să anulați această operație, faceți clic pe **Anulare**.

23.3.3. Pasul 3/3 - Examinați rezultatele

După ce toate fişierele au fost şterse, va apărea o nouă fereastră, unde puteți vedea rezultatele.

Rezultate

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

23.4. Curățarea regiștrilor Windows

Regiştrii Windows sunt o parte importantă a sistemelor de operare Windows. Aceştia reprezintă o bază de date care conține informații şi setări ce privesc componentele hardware şi sistemul de operare, aplicațiile instalate, utilizatorii, preferințele de pe calculatorul dumneavoastă şi altele

Multe aplicații editează chei în regiştrii Windows la instalare. La ştergerea sau dezinstalarea acestor programe, este posibil ca unele dintre cheile de regiştri asociate lor să nu fie şterse, ci să rămână în regiştrii Windows, încetinind sistemul şi chiar cauzând instabilitatea acestuia. La fel se întâmplă atunci când ştergeți scurtături către aplicații instalate sau fişiere ale acestora, precum şi în cazul driverelor corupte.

Pentru a curăța regiştrii Windows şi a îmbunătăți performanțele sistemului dumneavostră, utilizați programul asistent de curățare a regiştrilor. Acesta scanează regiştrii Windows şi şterge cheile de regiştri nevalide.

Pentru a curăța regiştrii Windows, urmați aceşti paşi:

1. În modul avansat, faceți clic pe **Optimizare PC** în meniul din stânga.
2. Faceți clic pe butonul **Execută acum** corespunzător funcției Curățare regiştri.
3. Urmați programul asistent în patru paşi.

23.4.1. Pasul 1/4 - Inițiați scanarea

Aici puteți inița scanarea regiştrilor.

Stare

Puteți vedea când a fost rulat ultima oară programul asistent şi recomandarea BitDefender.

Faceți clic pe **Înainte**.

23.4.2. Pasul 2/4 - Scanare...

Programul asistent va începe scanarea regiştrilor Windows.

Scanare...

Puteți vedea ultima cheie de regiştri scanată şi statisticile aferente.

Aşteptați ca scanarea cheilor de regiştri să fie finalizată. Dacă doriți să anulați această operație, faceți clic pe **Anulare**.

Notă
Dacă doriți oprirea scanării, faceți clic pe **Opreşte**. Veți sări peste următorul pas.

23.4.3. Pasul 3/4 - Selectați acțiunea

După finalizarea scanării cheilor de regiştri, va apărea o nouă fereastră, unde puteți vedea rezultatele.

Notă
Dacă nu au fost detectate probleme sau dacă ați ales să opriți scanarea, veți sări acest pas.

Acțiuni

Puteți vedea toate cheile de regiştri orfane sau nevalide detectate. Informații detaliate sunt furnizate despre fiecare cheie de regiştri (nume, valoare, prioritate, categorie).

Cheile de regiştri sunt grupate în funcție de locația lor în regiştrii Windows:

Categorie	*Descriere*
Locații aplicații	Chei de regiştri care conțin informații despre calea către aplicațiile instalate pe calculatorul dumneavoastră. Cheile nevalide au atribuite o prioritate scăzută, ceea ce înseamnă că le puteți şterge fără a le mai analiza.
Extensii de fişier	Chei de regiştri care conțin informații despre extensiile de fişier înregistrate pe calculatorul dumneavoastră. Aceste chei de regiştri sunt utilizate în mod obişnuit pentru a menține asocierile de fişiere (pentru a asigura deschiderea programului corect atunci când deschideți un fişier prin intermediul Windows Explorer). De

Categorie	Descriere
	exemplu, o astfel de cheie de regiştri permite Windows să deschidă un fişier `.doc` în Microsoft Word. Cheile nevalide au atribuite o prioritate scăzută, ceea ce înseamnă că le puteţi şterge fără a le mai analiza.
DLL-uri partajate	Chei de regiştri care conţin informaţii despre locaţia DLL-urilor (librăriilor de legături dinamice) partajate. DLL-urile conţin funcţii care sunt utilizate de aplicaţiile instalate pentru a executa anumite sarcini. Acestea pot fi partajate între mai multe aplicaţii pentru a reduce cerinţele de memorie şi spaţiu pe disc. Aceste chei de regiştri devin nevalide atunci când DLL-ul indicat este mutat în altă locaţie sau şters complet (acest lucru se întâmplă de obicei atunci când dezinstalaţi un program). Cheile nevalide au atribuite o prioritate medie, ceea ce înseamnă că ştergerea lor poate avea un impact negativ asupra sistemului.

Pentru a gestiona mai uşor procesul de curăţare, puteţi selecta o categorie din meniu.

Puteţi alege să ştergeţi toate cheile nevalide din categoria selectată sau doar unele dintre acestea. Dacă bifaţi **Şterge toate cheile**, toate cheile detectate vor fi şterse. Dacă doriţi să ştergeţi doar anumite chei, bifaţi opţiunea **Şterge** corespunzătoare cheilor respective.

Notă
În mod implicit, toate cheile nevalide detectate vor fi şterse.

Faceţi clic pe **Înainte**.

23.4.4. Pasul 4/4 - Examinaţi rezultatele

Aici puteţi vedea rezultatele scanării efectuate de programul asistent.

Rezultate

Dacă nu ați ales să ştergeți toate cheile, va fi afişat un mesaj de avertisment. Vă recomandăm să revedeți problemele respective.

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

23.5. Recuperarea regiştrilor curățați

Câteodată, după curățarea regiştrilor, pot apărea probleme în funcționarea sistemului de operare sau a unor aplicații, din cauza unor chei de regiştri lipsă. Acest lucru poate fi cauzat de ştergerea unor chei de regiştri folosite în comun de mai multe programe în timpul ultimei curățiri a regiştrilor sau de alte chei şterse. Pentru a rezolva această problemă trebuie să recuperați regiştrii curățați.

Pentru a reveni la configurația regiştrilor de dinainte de curățare, urmați aceşti paşi:

1. În modul avansat, faceți clic pe **Optimizare PC** în meniul din stânga.
2. Faceți clic pe butonul **Execută acum** corespunzător funcției Recuperare regiştri.

3. Urmați programul asistent în doi paşi.

Important
Doar utilizatorii cu drepturi administrative pe sistem pot recupera regiştrii curățați.

23.5.1. Pasul 1/2 - Inițiați recuperarea regiştrilor

Aici puteți inițiа recuperarea regiştrilor.

Stare

Puteți vedea lista momentelor de timp când au fost curățați regiştrii Windows. Selectați momentul de timp corespunzător configurației regiştrilor Windows la care doriți să reveniți.

Pentru a reveni la configurația regiştrilor Windows de la momentul selectat, faceți clic pe **Înainte**.

Avertisment
Recuperarea regiştrilor curăţaţi poate duce la suprascrierea cheilor de regiştri editate de la ultima curăţare.

23.5.2. Pasul 2/2 - Examinați rezultatele

Aici puteți vedea dacă recuperarea a fost efectuată cu succes.

Rezultate

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

23.6. Depistarea fișierelor duplicat

Fişierele duplică consumă spațiul hard discului dumneavoastră. Gândiți-vă doar că ați avea acelaşi fişier `.mp3` stocat în trei locații diferite.

Pentru a detecta şi şterge fişierele duplicat de pe calculatorul dumneavostră, puteți utiliza programul asistent de depistare a duplicatelor. În acest fel puteți gestiona mai bine spațiul liber de pe hard discul dumneavoastră.

Pentru a descoperi fişiere duplicat pe calculatorul dumneavoastră, urmaţi aceşti paşi:

1. În modul avansat, faceţi clic pe **Optimizare PC** în meniul din stânga.
2. Faceţi clic pe butonul **Execută acum** corespunzător funcţiei Căutare duplicate.
3. Urmaţi programul asistent în patru paşi.

23.6.1. Pasul 1/4 - Selectaţi locaţia căutării

Aici puteţi specifica unde să fie căutate fişiere duplicat.

Locaţie căutare

Faceţi clic pe **Caută** şi selectaţi o locaţie unde programul asistent să caute fişiere duplicat. Calea către locaţia selectată va apărea în coloana **Cale**. Dacă vă răzgândiţi în legătură cu locaţia, faceţi clic pe butonul **Şterge** de lângă aceasta.

Notă
Puteţi selecta una sau mai multe locaţii.

Faceți clic pe **Înainte**.

23.6.2. Pasul 2/4 - Căutare...

Programul asistent va începe să caute fişiere duplicat.

Căutare...

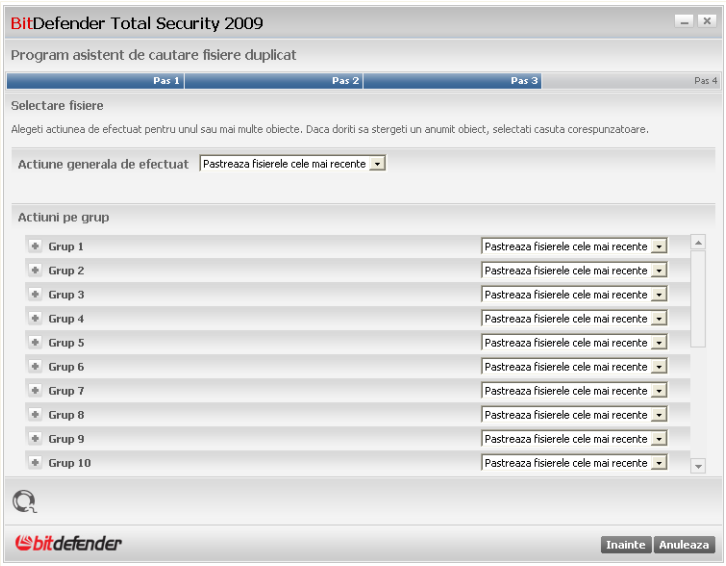
Puteți vedea stadiul şi statisticile căutării.

Aşteptați să fie finalizată căutarea de fişiere duplicat. Dacă doriți să anulați această operație, faceți clic pe **Anulare**.

23.6.3. Pasul 3/4 - Selectați acțiunea

După ce căutarea a fost finalizată, va apărea o nouă fereastră, unde puteți specifica ce acțiuni să fie luate asupra fişierelor duplicat detectate.

Notă
Dacă nu au fost detectate fişiere duplicat, veți sări acest pas.



Acțiuni

Fişierele duplicat detectate sunt organizate şi afişate în grupuri. Dacă faceți clic pe căsuța corespunzătoare unui grup, puteți vedea informații detaliate despre fişierele duplicat (calea completă, dimensiunea, data creării şi modificării).

Puteți alege o acțiune globală care să fie aplicată tuturor fişierelor duplicat detectate sau puteți alege acțiuni care să fie aplicate pe grupuri de fişiere duplicat. Următoarele acțiuni sunt disponibile pe meniu:

Acțiune	Descriere
Păstrează cel mai recent fişier	Va fi păstrat cel mai recent duplicat, în timp ce celelalte vor fi şterse.
Păstrează cel mai vechi fişier	Va fi păstrat cel mai vechi duplicat, în timp ce celelalte vor fi şterse.
Nicio acțiune	Nu se va aplica nicio acțiune fişierelor detectate.

Dacă doriți să aplicați o acțiune globală tuturor obiectelor dintr-un grup, selectați acțiunea dorită din meniul corespunzător. Dacă doriți ca doar anumite fişiere dintr-un grup să fie şterse, bifați opțiunea **Şterge** corespunzătoare fişierelor respective.

Notă

Acțiunea globală nu va suprascrie acțiunea aleasă pentru anumite grupuri sau fişiere. Aceasta înseamnă, de exemplu, că dacă setați ca acțiune globală **Păstrează cel mai recent fişier**, dar specificați să nu fie aplicată nicio acțiune unui anumit grup, atunci acțiunea globală va fi aplicată tuturor grupurilor cu excepția acestuia.

Faceți clic pe **Înainte**.

23.6.4. Pasul 4/4 - Examinați rezultatele

Aici puteți vedea rezultatele scanării după fişiere duplicat.

Rezultate

Faceți clic pe **Execută din nou** pentru a porni o nouă căutare de fişiere duplicat sau pe **OK** pentru a închide fereastra.

24. 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.

24.1. 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 şi 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 şi la ieşire) sunt permise în mod automat, indiferent de portul şi protocolul utilizat.
- Actualizările nu sunt efectuate în mod implicit.

  Notă
  Pentru a modifica această setare, mergeți la Actualizare>Setări şi debifați căsuța **Nu actualiza dacă este activat modul pentru jocuri**.

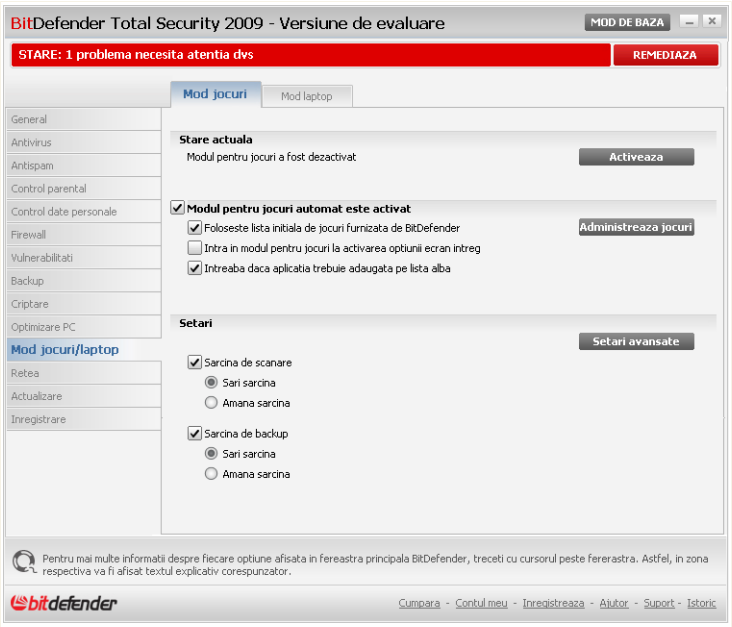
- Sarcinile de scanare programate sunt dezactivate în mod implicit.
- Sarcinile de backup programate sunt dezactivate în mod implicit.

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 ieşiți din modul pentru jocuri atunci când ați terminat jocul (puteți utiliza aceeaşi combinația de taste implicită `Ctrl+Alt+Shift+G`).

Notã

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

Pentru a configura modul pentru jocuri, mergeți la **Mod pentru jocuri / laptop>Mod pentru jocuri** în modul avansat.



Modul pentru jocuri

În partea de sus a secțiunii, puteți vedea starea modului pentru jocuri. Faceți clic pe **Intră în modul pentru jocuri** sau pe **Ieşi din modul pentru jocuri** pentru a schimba starea curentă.

24.1.1. Configurarea modului pentru jocuri automat

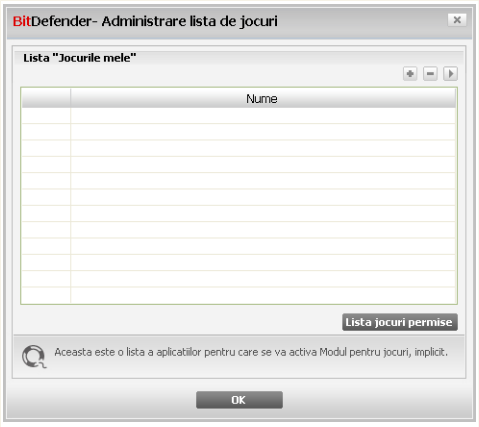
Modul pentru jocuri automat permite BitDefender să intre automat în modul pentru jocuri atunci când este detectat un joc. Puteți configura următoarele opțiuni:

- **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** şi apoi pe **Afişează jocuri permise**.
- **Întră în modul pentru jocuri la intrarea în full screen** - pentru a intra automat în modul pentru jocuri când o aplicație ocupă întregul ecran (full screen).
- **Adaugă aplicația la lista de jocuri?** - pentru a vi se solicita adăugarea unei noi aplicații la lista de jocuri atunci când aceasta iese din full screen. Adăugând o aplicație nouă la lista de jocuri, data viitoare când o veți porni 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**.

24.1.2. Administrarea listei de jocuri

BitDefender intră automat în modul pentru jocuri atunci când porniți o aplicație din lista de jocuri. Pentru a vedea şi 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 **Afişează jocuri permise**.
- După ieşirea 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 şi programele de vizionat filme.

Pentru a administra lista de jocuri, puteți utiliza butoanele plasate în partea de sus a tabelului:

- **Add** - add a new application to the game list.
- **Remove** - remove an application from the game list.
- **Edit** - edit an existing entry in the game list.

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.

24.1.3. Configurarea setărilor modului pentru jocuri

Pentru a configura executarea sarcinilor programate, utilizați aceste opțiuni:

- **Sarcină de scanare** - pentru a bloca executarea sarcinilor de scanare programate în modul pentru jocuri. Puteți selecta una dintre următoarele opțiuni:

Opțiune	Descriere
Sări peste sarcină	Sarcina programată nu este executată deloc.
Amână sarcina	Execută sarcina imediat după ieşirea din modul pentru jocuri.

- **Sarcină de backup** - pentru a bloca executarea sarcinilor de backup programate în modul pentru jocuri. Puteți selecta una dintre următoarele opțiuni:

Opțiune	Descriere
Sări peste sarcină	Sarcina programată nu este executată deloc.
Amână sarcina	Execută sarcina imediat după ieşirea din modul pentru jocuri.

Pentru a dezactiva automat firewallul BitDefender în modul pentru jocuri, urmați aceşti paşi:

1. Faceți clic pe **Setări avansate**. Va apărea o nouă fereastră.
2. Selectați căsuța **Nu utiliza firewallul**.
3. Faceți clic pe **OK** pentru a salva modificările.

24.1.4. 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 aceşti paşi:

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` şi `Alt` şi să tastați `D`.
3. Faceți clic pe **OK** pentru a salva modificările.

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

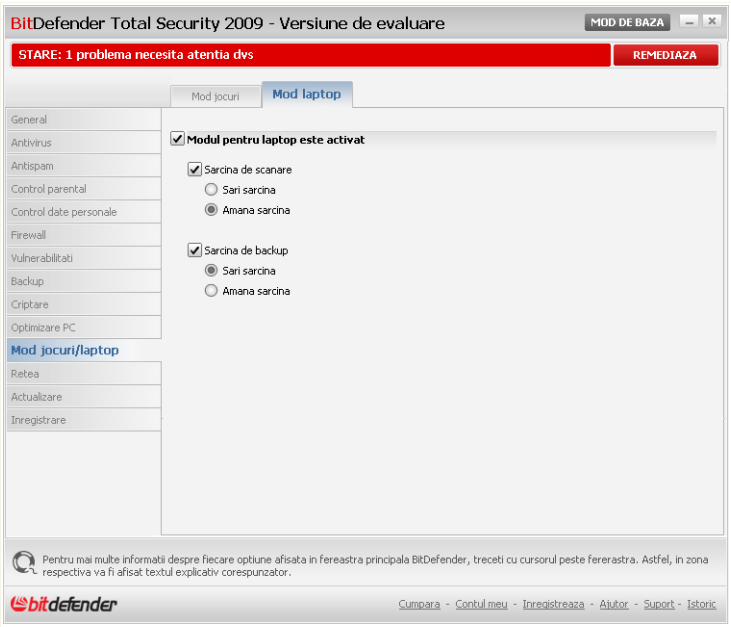
24.2. Modul pentru laptop

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 şi 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 pentru jocuri / laptop>Mod pentru laptop** în modul avansat.



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.

24.2.1. Configurarea setărilor modului pentru laptop

Pentru a configura executarea sarcinilor programate, utilizați aceste opțiuni:

- **Sarcină de scanare** - pentru a bloca executarea sarcinilor de scanare programate în modul pentru laptop. Puteți selecta una dintre următoarele opțiuni:

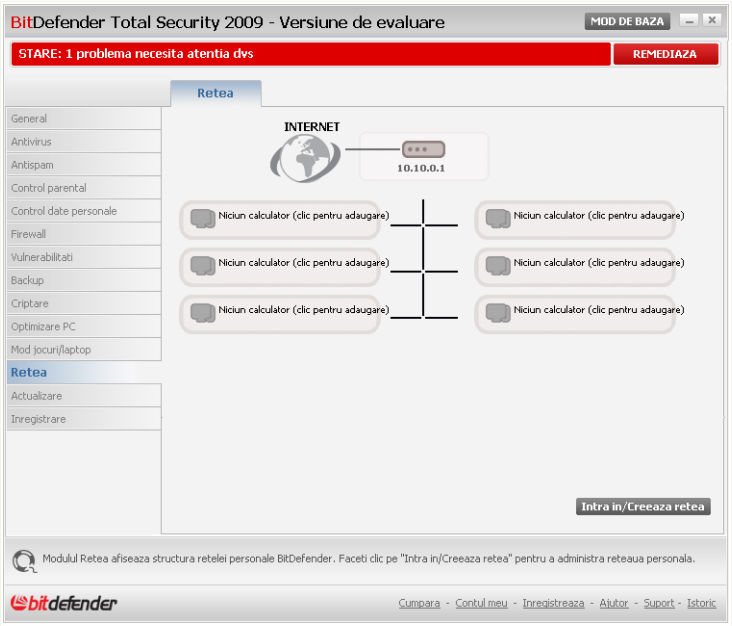
Opțiune	Descriere
Sări peste sarcină	Sarcina programată nu este executată deloc.
Amână sarcina	Execută sarcina imediat după ieşirea din modul pentru laptop.

- **Sarcină de backup** - pentru a bloca executarea sarcinilor de backup programate în modul pentru laptop. Puteți selecta una dintre următoarele opțiuni:

Opțiune	Descriere
Sări peste sarcină	Sarcina programată nu este executată deloc.
Amână sarcina	Execută sarcina imediat după ieşirea din modul pentru laptop.

25. Rețea

Modulul Rețea vă permite să administrați produsele BitDefender instalate pe calculatoarele personale de pe un singur calculator.



Hartă rețea

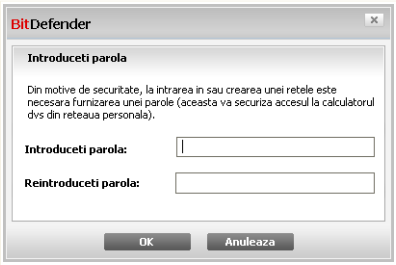
Pentru a putea administra produsele BitDefender instalate pe calculatoarele personale, trebuie să urmați aceşti paşi:

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 şi intrați în rețea (setați parola).
3. Întoarceți-vă la calculatorul dumneavoastră şi adăugați calculatoarele pe care doriți să le administrați.

25.1. Intrarea în rețeaua BitDefender

Pentru a în rețeaua BitDefender personală, urmați aceşti paşi:

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



Configurare parolă

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

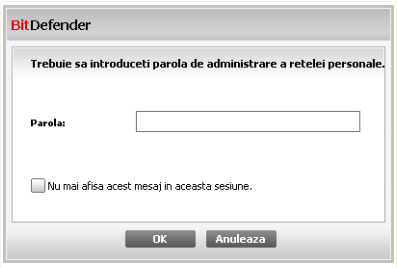
Puteți vedea numele calculatorului apărând pe harta rețelei.

25.2. 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.

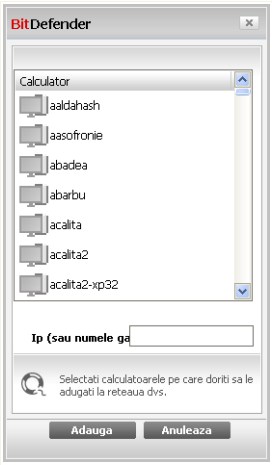
Pentru a adăuga un calculator la rețeaua BitDefender personală, urmați aceşti paşi:

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



Introducere parolă

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



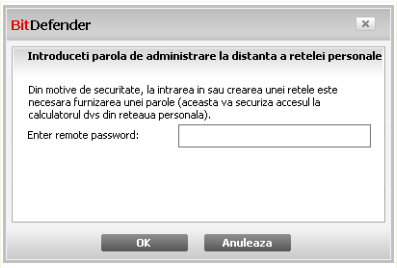
Adaugare calculator

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.



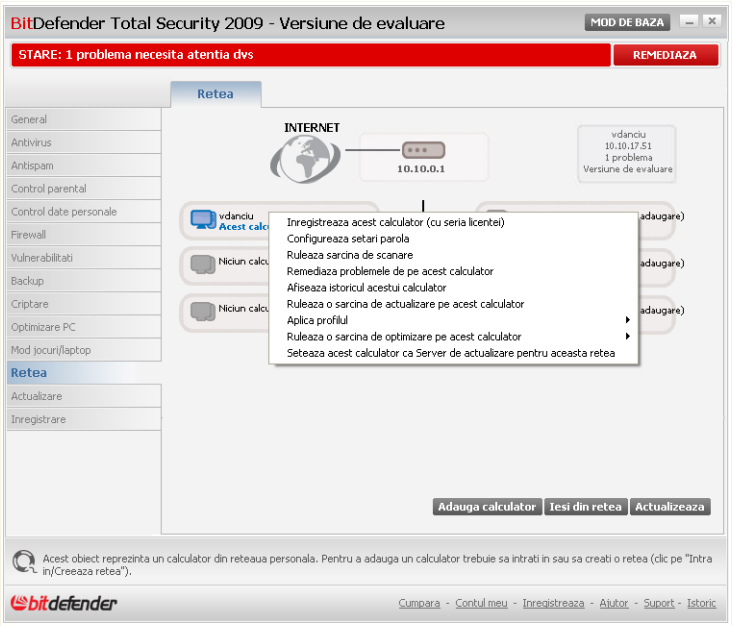
Autentificare

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.

25.3. Administrarea rețelei BitDefender

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



Hartă rețea

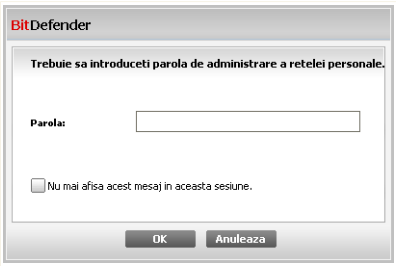
Dacă plasați cursorul mouse-ului deasupra unui calculator de pe harta rețelei, puteți vedea informații sumare despre acesta (nume, adresă IP, numărul de probleme care afectează securitatea sistemului, starea înregistrării).

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.

- **Înregistrează acest calculator**
- **Configurează parola pentru setări**
- **Execută o sarcină de scanare**
- **Repară probleme pe acest calculator**
- **Afişează evenimentele de pe acest calculator**
- **Execută o actualizare pe acest calculator acum**

- **Aplică profil**
- **Execută o sarcină de optimizare pe acest calculator**
- **Setați acest calculator ca server de actualizare al acestei rețele**

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 şi 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.

26. Actualizare

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

Dacă sunteţi conectat la Internet, prin bandă largă sau ADSL, BitDefender se ocupă singur de actualizări. Implicit, BitDefender caută actualizări când deschideţi calculatorul şi apoi la fiecare **oră**.

Dacă o actualizare este disponibilă, vi se va cere să confirmaţi actualizarea sau aceasta va fi realizată automat, în funcţie 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 funcţionarea produsului şi, în acelaşi timp, orice vulnerabilitate va fi exclusă.

Actualizările sunt de mai multe tipuri:

- **Actualizări pentru motoarele Antivirus** - pentru că tot timpul apar noi ameninţări, fişierele ce conţin semnăturile de viruşi trebuie actualizate pentru a asigura protecţie permanentă, la zi, împotriva acestora. Acest tip de actualizare se mai numeşte **Actualizare definiţii viruşi**.
- **Actualizări ale motoarelor Antispam** - se vor adăuga noi reguli filtrelor euristic şi URL şi noi imagini filtrului de imagine. Astfel, eficienţa motorului Antispam va creşte. Acest tip de actualizare se mai numeşte **Actaulizare Antispam**.
- **Actualizări ale motoarelor antispyware** - se vor adăuga noi semnături de spyware la baza de date. Acest tip de actualizare se mai numeşte **Actualizare Antispyware**.
- **Actualizare de produs** - la lansarea unei noi versiuni de produs, noi caracteristici şi tehnici de scanare sunt introduse pentru a îmbunătăţi performanţele produsului. Acest tip de actualizare se mai numeşte **Upgrade Produs**.

26.1. Actualizarea Automată

Pentru a vedea informaţii referitoare la actualizare şi iniţia actualizări automate, mergeţi la **Actualizare>Actualizare** în modul avansat.

Actualizarea Automată

Aici puteți vedea când au fost realizate ultima căutare de actualizări şi ultima actualizare, precum şi informații despre ultima actualizare realizată (dacă a fost reuşită sau dacă au apărut erori). De asemenea, sunt afişate informații despre versiunea curentă a motorului de scanare şi 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.

Puteți obține semnăturile aplicațiilor malițioase deținute de produsul dumneavoastră BitDefender făcând clic pe **Afişează listă viruşi**. Un fişier HTML care conține toate semnăturile disponibile va fi creat şi deschis într-un browser. Puteți căuta prin baza

de date după o anumită semnătură sau puteți face clic pe **Lista de viruşi BitDefender** pentru a accesa baza de semnături online a BitDefender.

26.1.1. Cererea unei actualizări

Actualizarea automată poate fi realizată oricând făcând clic pe **Actualizează acum**. Acest tip de actualizare este cunoscut şi ca **actualizare la cererea utilizatorului**.

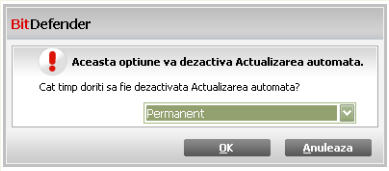
Modulul **Actualizare** se va conecta la serverul de actualizare BitDefender şi va verifica dacă sunt disponibile noi semnături. Dacă sunt detectate noi semnături, în funcție de opțiunile setate în secțiunea Setări actualizare la cerere, vi se va cere să confirmați actualizarea sau aceasta va fi realizată 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.

26.1.2. Dezactivarea actualizării automate

Dacă doriți să dezactivați actualizarea automată, va apărea o fereastră de avertizare.



Dezactivează actualizarea automată

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.

26.2. Setări 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, şi va instala actualizările disponibile fără a vă mai avertiza.

Pentru a configura setările de actualizare şi a gestiona setările proxy, faceți clic pe **Actualizare>Setări** în modul avansat.

Setări actualizare

Setările de actualizare sunt grupate în patru categorii (**Setări locație de actualizare**, **Setări actualizare automată**, **Setări actualizare la cerere** şi **Setări avansate**). Fiecare categorie va fi descrisă separat.

26.2.1. 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 şi mai rapidă, puteți configura două locații de actualizare: o **Locație de actualizare principală** şi 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 şi 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, bifați **Utilizez proxy** şi apoi faceți clic pe **Gestionare proxy** pentru a configura setările proxy. Pentru mai multe informații, consultați "*Administrarea proxy-urilor*" (p. 397).

26.2.2. 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 **Interval de timp**. Implicit, intervalul de timp 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 şi 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.

26.2.3. 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.

26.2.4. 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 işi va continua funcționarea folosind fişierele vechi până când utilizatorul va reporni calculatorul din proprie inițiativă. Utilizatorului nu i se va cere repornirea calculatorului şi 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 desfăşurare. 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.

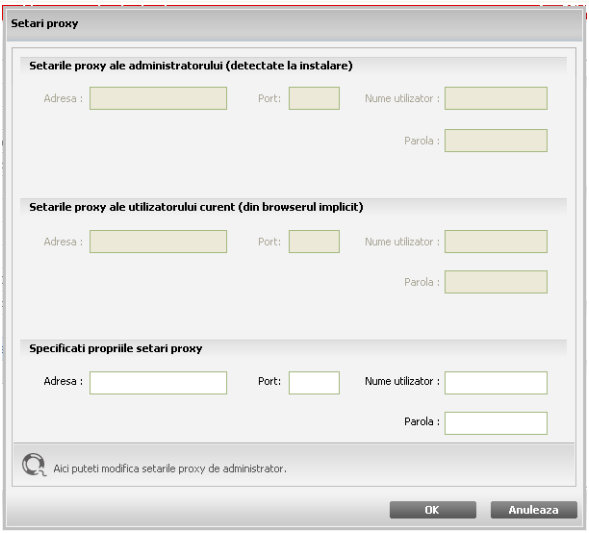
- **Nu actualiza dacă este activat modul pentru jocuri** - BitDefender nu se va actualiza dacă funcționează în modul pentru jocuri. Astfel, puteți minimiza influența produsului asupra performanțelor sistemului în timpul jocului.

26.2.5. 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.

Notã
Setările proxy pot fi configurate doar de utilizatori cu drepturi administrative pe calculator sau de către utilizatori care cunosc parola produsului.

Pentru a gestiona setările proxy, faceți clic pe **Gestionare proxy**. Va apărea o nouă fereastră.



Fereastra de gestionare a setărilor proxy

Există trei seturi de setări proxy:

- **Setările proxy ale administratorului (detectate la instalare)** - setări proxy detectate pe contul administratorului în timpul instalării şi care pot fi configurate doar dacă sunteți logat pe acel cont. Dacă serverul proxy necesită un nume de utilizator şi o parolă pentru autentificare, atunci va trebui să le specificați în câmpurile corespunzătoare.
- **Setările proxy ale utilizatorului curent (din browserul implicit)** - setări proxy ale utilizatorului curent, extrase din browserul implicit. Dacă serverul proxy necesită un nume de utilizator şi o parolă pentru autentificare, atunci va trebui să le specificați în câmpurile corespunzătoare.

Notă
Browserele web suportate sunt Internet Explorer, Mozilla Firefox şi Opera. Dacă utilizaţi un alt browser în mod implicit, BitDefender nu va putea obţine setările proxy ale utilizatorului curent.

- **Specificaţi propriile setări proxy** - setări proxy pe care le puteţi configura dacă sunteţi logat ca administrator.

  Următoarele setări trebuie specificate:
  - **Adresă** - introduceţi adresa IP a serverului proxy.
  - **Port** - introduceţi portul folosit BitDefender pentru a se conecta la serverul proxy.
  - **Utilizator** - introduceţi un nume de utilizator recunoscut de proxy.
  - **Parolă** - introduceţi 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 reuşi conexiunea.

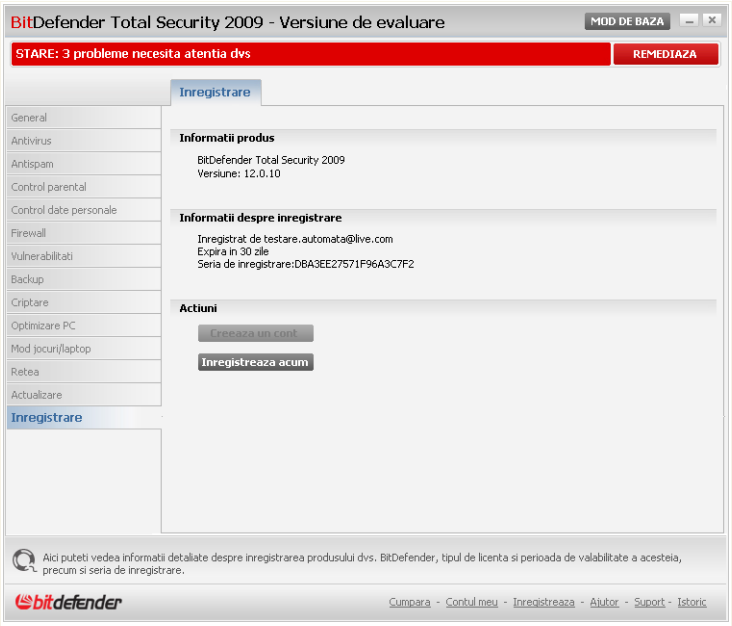
Mai întâi, va fi utilizat setul conţinând propriile dumneavoastre setări proxy pentru conectarea la Internet. Dacă acesta nu merge, vor fi încercate în continuare setările proxy detectate la instalare. În sfârşit, dacă nici acestea nu sunt bune, vor fi extrase setările proxy ale utilizatorului curent din browserul implicit şi vor fi folosite pentru conectarea la Internet.

Faceţi clic pe **OK** pentru a salva modificările şi închide fereastra.

Faceţi clic pe **Salvare** pentru a salva modificările sau pe **Implicit** pentru a încărca setările standard.

27. Înregistrare

Pentru a afla informații complete despre produsul dumneavoastră BitDefender şi despre starea înregistrării, mergeți la **Înregistrare** în modul avansat.



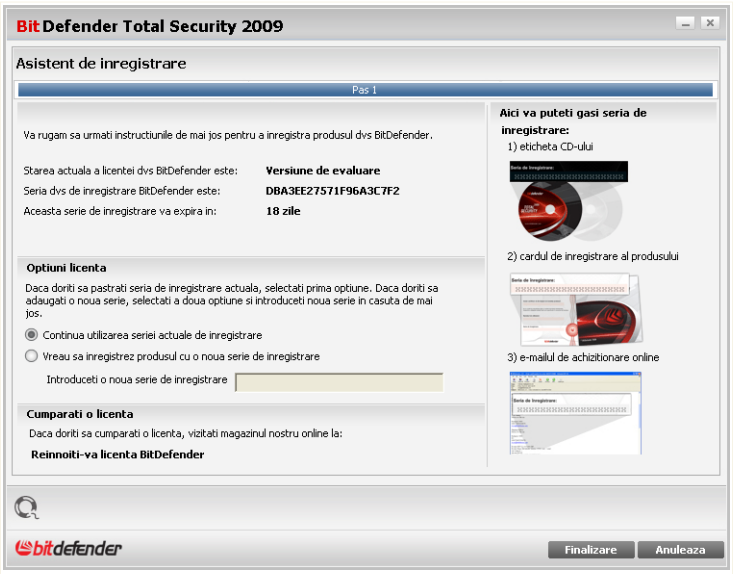
Înregistrare

Această secțiune afişează:

- **Informații despre produs**: produsul BitDefender şi 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 şi câte zile au mai rămas până la expirarea licenței.

27.1. Înregistrarea BitDefender Total Security 2009

Faceți clic pe **Înregistrează acum** pentru a deschide fereastra de înregistrare a produsului.



Înregistrare

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

Dacă perioada de evaluare nu a expirat şi doriți să evaluați produsul în continuare, selectați **Continuă evaluarea produsului**.

Pentru a înregistra BitDefender Total Security 2009:

1. Selectați **Vreau să înregistrez produsul cu o nouă serie**.
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 şi a cumpăra una.

Faceți clic pe **Finalizare**.

27.2. Crearea unui cont BitDefender

Contul BitDefender oferă acces la suport tehnic gratuit, oferte speciale şi promoții. Daca v-ați pierdut seria de înregistrare BitDefender, puteți accesa contul dumneavoastră la http://myaccount.bitdefender.com pentru a o recupera.

Dacă nu ați creat încă un cont BitDefender, faceți clic pe **Creează cont** pentru a deschide fereastra de înregistrare a contului.

Creare cont

Dacă nu doriți să creați un cont BitDefender în acest moment, selectați **Sari peste înregistrare** şi faceți clic pe **Finalizare** Altfel, continuați în funcție de situația dumneavoastră actuală:

- “Nu am un cont BitDefender” (p. 403)
- “Deja am un cont BitDefender” (p. 404)

Nu am un cont BitDefender

Selectați **Creează un nou cont BitDefender** şi furnizați informațiile cerute. Informațiile furnizate aici vor rămâne confidențiale.

- **E-mail** - introduceți adresa de e-mail.
- **Parolă** - introduceți o parolă pentru contul dumneavoastră BitDefender. Parola trebuie să conțină minim şase caractere.
- **Reintroduceți parola** - introduceți parola din nou.

- **Prenume** - introduceți prenumele dumneavoastră.
- **Nume** - introduceți numele dumneavoastră de familie.
- **Țara** - selectați țara în care locuiți.

Notă
Folosiți adresa de e-mail şi parola pentru a vă accesa contul dumneavoastră la adresa http://myaccount.bitdefender.com.

Pentru a crea un cont trebuie mai întâi să vă activați adresa de e-mail. Verificați-vă adresa de e-mail şi urmați instrucțiunile din e-mailul trimis de serviciul de înregistrare BitDefender.

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

- **Vreau sa primesc toate mesajele de la BitDefender**
- **Vreau sa primesc numai cele mai importante mesaje**
- **Nu vreau sa primesc niciun mesaj**

Faceți clic pe **Finalizare**.

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 dumneavoastră.

Dacă aveți deja un cont activ, dar BitDefender nu l-a detectat, selectați **Accesează un cont BitDefender existent** şi furnizați adresa de e-mail şi parola contului dumneavoastră.

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

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

- **Vreau sa primesc toate mesajele de la BitDefender**
- **Vreau sa primesc numai cele mai importante mesaje**
- **Nu vreau sa primesc niciun mesaj**

Faceți clic pe **Finalizare**.

Obținere ajutor

28. Suport

BitDefender se străduieşte să ofere clienţilor săi un nivel cât mai ridicat în ceea ce priveşte rapiditatea şi calitatea suportului tehnic. Centrul de suport (cu care puteţi lua legătura prin adresa indicată mai jos) este actualizat continuu. Aici vă sunt oferite răspunsurile la întrebările dumneavoastră în cel mai scurt timp.

La BitDefender, preocuparea pentru economisirea timpului şi banilor clienţilor prin oferirea celor mai avansate produse la preţuri rezonabile a fost dintotdeauna o prioritate. Mai mult, considerăm că o afacere de succes se bazează pe o bună comunicare şi dedicare în suportul acordat clienţilor.

Sunteţi binevenit oricând să cereţi ajutor la suport@bitdefender.ro. Pentru un răspuns prompt, includeţi în e-mail cât mai multe detalii despre produsul BitDefender pe care-l deţineţi, despre sistemul dumneavoastră şi descrieţi cât mai exact problema.

28.1. BitDefender Knowledge Base

BitDefender Knowledge Base este o bază online de informaţii despre produsele BitDefender. Stochează, într-un format accesibil, rapoarte ale echipelor de suport şi dezvoltare cu privire la rezultatele suportului tehnic continuu şi ale activităţilor de eliminare a bug-urilor BitDefender împreună cu articole mai generale despre prevenţia viruşilor, administrarea soluţiilor BitDefender şi explicaţii detaliate, şi multe alte articole.

BitDefender Knowledge Base este pusă la dispoziţia publicului. Această multitudine de informaţii reprezintă încă o cale de a oferi clienţilor BitDefender asistenţa tehnică de care au nevoie. Toate cererile valide de informaţii sau rapoarte despre bug-uri venind de la clienţii BitDefender ajung în cele din urmă în BitDefender Knowledge Base, ca rapoarte asupra eliminării bug-urilor, fişe de lucru sau articole informative pentru a suplimenta fişierele de suport ale produsului.

BitDefender Knowledge Base este disponibilă oricând la adresa http://kb.bitdefender.com.

28.2. Solicitarea ajutorului

28.2.1. Mergeţi la serviciul Web Self

Aveţi o întrebare? Experţii noştri în securitate vă stau la dispoziţie non-stop, oferindu-vă ajutor gratuit prin telefon, e-mail sau chat.

Utilizați linkurile de mai jos:

Engleză

http://www.bitdefender.com/site/KnowledgeBase/

Germană

http://www.bitdefender.com/de/KnowledgeBase/

Franceză

http://www.bitdefender.com/fr/KnowledgeBase/

Română

http://www.bitdefender.com/ro/KnowledgeBase/

Spaniolă

http://www.bitdefender.com/es/KnowledgeBase/

28.2.2. Deschideți o cerere de ajutor

Dacă doriți să faceți o cerere de ajutor şi să primiți ajutor prin e-mail, utilizați unul dintre linkurile următoare:

Engleză: http://www.bitdefender.com/site/Main/contact/1/
Germană: http://www.bitdefender.de/site/Main/contact/1/
Franceză: http://www.bitdefender.fr/site/Main/contact/1/
Română: http://www.bitdefender.ro/site/Main/contact/1/
Spaniolă: http://www.bitdefender.es/site/Main/contact/1/

28.3. Informații de contact

Comunicarea eficientă este cheia unei afaceri de succes. În ultimii 10 ani BitDefender a câştigat o reputație indisputabilă în depăşirea aşteptărilor clienților şi partenerilor, căutând în mod constant mijloace pentru o comunicare eficientă. Nu ezitați să ne contactați indiferent ce problemă sau întrebare ați avea.

28.3.1. Adrese Web

Departament de vânzări: sales@bitdefender.ro
Suport tehnic: suport@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 viruşi: 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.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

28.3.2. Filiale

Sucursalele BitDefender sunt pregătite să răspundă oricăror întrebări legate de aria lor de operare, atât în ce priveşte problemele comerciale cât şi pe cele generale. Adresele lor precum şi modul în care pot fi contactate sunt date mai jos.

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Telefon: 1-954-776-6262
Pagină web: http://www.bitdefender.com

Suport tehnic (doar pentru utilizatori înregistrați):
- E-mail: support@bitdefender.com
- Telefon gratuit:
  - Statele Unite: 1-888-868-1873
  - Canada: 1-866-947-1873

Serviciu clienți (doar pentru utilizatori înregistrați):
- E-mail: customerservice@bitdefender.com
- Telefon gratuit:
  - Statele Unite: 1-888-868-1873

- Canada: 1-866-947-1873

Germany

BitDefender GmbH
Airport Office Center
Robert - Bosch - Str. 2
59439 Holzwickede
Germany
Telefon: +49 (0)231 99 33 98 0
Email: info@bitdefender.com
Vânzări: sales@bitdefender.ro
Pagină web: http://www.bitdefender.com
Suport tehnic: support@bitdefender.com

Marea Britanie și Irlanda

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
Tel: +44 (0) 8451-305096
Email: info@bitdefender.com
Vânzări: sales@bitdefender.ro
Pagină web: http://www.bitdefender.co.uk
Suport tehnic: suport@bitdefender.ro

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2ª planta, 08006
Barcelona
Soporte técnico: soporte@bitdefender-es.com
Ventas: comercial@bitdefender-es.com
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

Romania

BITDEFENDER
Strada Preciziei nr. 24, West Gate Park, Clădirea H2, parter, sector 6

Bucureşti
Suport tehnic: suport@bitdefender.ro
Vânzări: sales@bitdefender.ro
Telefon suport: +40 21 3001226 (27,28,29)
Telefon vânzări: +40 21 2063470
Site produs: http://www.bitdefender.ro

BitDefender Rescue CD

29. Descriere generală

BitDefender Total Security 2009 este furnizat cu un CD de boot (BitDefender Rescue CD) capabil să scaneze şi dezinfecteze tot calculatorul fără a mai fi necesară pornirea sistemului de operare.

Este indicat să utilizaţi BitDefender Rescue CD oricând sistemul dumneavoastră de operare nu funcţionează corect din cauza infecţiei cu viruşi. Aceasta se întâmplă în general când nu folosiţi un produs antivirus.

Actualizarea definiţiilor de viruşi se face automat, fără intervenţia utilizatorului de fiecare dată când este pornit BitDefender Rescue CD.

BitDefender Rescue CD este o distribuţie Knoppix adaptată de BitDefender, care integrează cea mai recentă soluţie de securitate BitDefender pentru Linux într-un CD GNU/Linux Knoppix Live, oferind un antivirus pentru desktop care este capabil să scaneze şi să dezinfecteze hard discurile existente (incluzând partiţiile Windows NTFS). De asemenea, BitDefender Rescue CD poate fi utilizat pentru a restaura datele dumneavoastră importante atunci când nu puteţi porni Windowsul.

Notă
BitDefender Rescue CD poate fi descărcat de la această locaţie: http://download.bitdefender.com/rescue_cd/

29.1. Cerinţe de sistem

Înainte de a porni BitDefender Rescue CD, trebuie să vă asiguraţi că sistemul dumneavoastră îndeplineşte următoarele cerinţe.

Tip procesor
Procesor compatibil cu x86, minimum 166 MHz, dar nu aşteptaţi performanţe ridicate în acest caz. Un procesor de generaţie i686, la 800MHz, constituie o alegere mai bună.

Memorie RAM
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 şi un BIOS capabil să-l pornească.

Conexiune Internet
Deşi BitDefender Rescue CD va rula fără conexiune Internet, procedurile de actualizare vor necesita un link HTTP activ, chiar şi printr-un server proxy. De aceea, pentru o protecție actualizată, conexiunea Internet este o CERINȚĂ.

Rezoluție grafică
Placă video standard compatibilă SVGA.

29.2. Soft inclus

BitDefender Rescue CD include următoarele pachete soft.

Xedit
Acesta este un editor text de fişiere.

Vim
Acesta este un editor text de fişiere avansat, oferind evidențierea sintaxei, o interfață grafică şi multe altele. Pentru mai multe informații, consultați pagina web a Vim.

Xcalc
Acesta este un calculator.

RoxFiler
RoxFiler este manager de fişiere grafic, rapid şi avansat.

Pentru mai multe informații, consultați pagina web a RoxFiler.

MidnightCommander
GNU Midnight Commander (mc) este un manager de fişiere în mod text.

Pentru mai multe informații, consultați pagina web a MC.

Pstree
Pstree afişează procesele care rulează.

Top
Top afişează sarcinile Linux.

Xkill
Xkill opreşte un program care rulează în X.

Partition Image
Partition Image vă ajută să salvați partiții în format EXT2, Reiserfs, NTFS, HPFS, FAT16 şi FAT32 într-un fişier 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 şi 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 afişează 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 afişează statistici referitoare la traficul TCP/IP la intrare şi la ieşire.

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 afişează 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 ieşirea 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.

30. Instrucțiuni BitDefender Rescue CD

Acest capitol conține informații despre pornirea şi oprirea BitDefender Rescue CD, scanarea calculatorului dumneavoastră după aplicații malițioase precum şi salvarea datelor de pe un PC cu Windows compromis pe un dispozitiv mobil. Totuşi, utilizând aplicațiile software care sunt oferite pe CD, puteți executa numeroase alte sarcini, descrierea acestora fiind departe de scopul acestui manual de utilizare.

30.1. Pornirea BitDefender Rescue CD

Pentru a porni cd-ul, setați BIOS-ul calculatorului dumneavoastră să demareze de pe cd, aşezați cd-ul în drive şi reporniți calculatorul. Asigurați-vă că poate fi pornit calculatorul dumneavoastră de pe cd.

Aşteptați până apare următorul ecran şi urmați instrucțiunile pentru a porni BitDefender Rescue CD.

Notă
Selectați limba pe care doriți să o utilizați pentru Rescue CD din lista disponibilă.

Ecran la pornirea sistemului

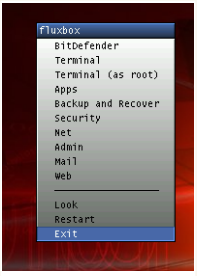
La pornirea sistemului, se face automat actualizarea semnăturilor de viruşi. Procesul poate lua ceva timp.

La finalizarea procesului de pornire veți vedea următorul desktop. Acum puteți începe să utilizați BitDefender Rescue CD.

Desktopul

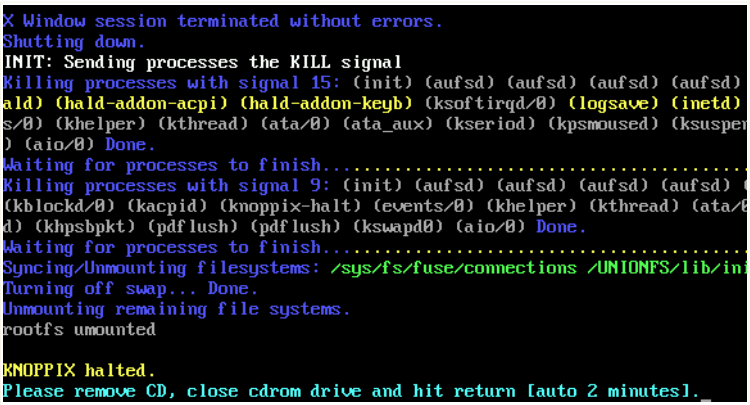
30.2. Oprirea BitDefender Rescue CD

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

30.3. 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 paşi pentru a realiza procesul de scanare.

1. Puteți vedea stadiul şi statisticile scanării (viteza de scanare, timpul scurs de la începutul scanării, numărul obiectelor scanate / infectate / suspecte / ascunse şi 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 afişate pe grupuri. Faceţi clic pe căsuţa cu “+” pentru a deschide un grup sau pe căsuţa cu “-” pentru a închide un grup.

Puteţi alege o acţiune globală care să fie luată asupra fiecărui grup de probleme sau puteţi alege acţiuni separate pentru fiecare problemă în parte.

3. Puteţi vedea un rezumat al rezultatelor.

Dacă doriţi să scanaţi doar un anumit director, procedaţi în felul următor:

Navigaţi printre fişiere, faceţi clic-dreapta pe fişierul sau directorul dorit şi selectaţi **Send to**. Apoi alegeţi **BitDefender Scanner**.

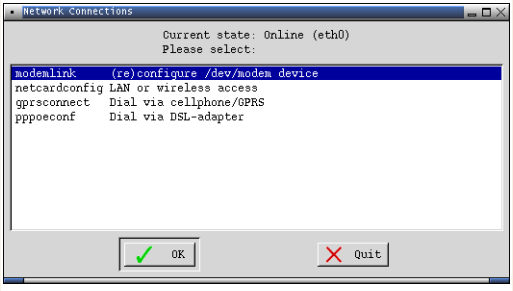
Sau puteţi iniţializa următoarea comandă de la un terminal. **BitDefender Antivirus Scanner** va începe cu fişierul sau directorul selectat ca locaţie implicită de scanare.

```
# bdscan /path/to/scan/
```

30.4. Cum configurez conexiunea Internet?

Dacă sunteţi într-o reţea DHCP şi aveţi un card de reţea ethernet, conexiunea Internet ar trebui să fie deja detectată şi configurată. Pentru configurare manuală, urmaţi paşii de mai jos.

1. Faceţi dublu-clic pe iconiţa Network Connections (Conexiuni reţea) de pe desktop. Va apărea următoarea fereastră:



Network Connections (Conexiuni reţea)

2. Selectaţi tipul conexiunii utilizate şi faceţi clic pe OK.

Conexiune	Descriere
modemlink	Selectați acest tip de conexiune dacă folosiți un modem şi o linie telefonică pentru acces la Internet.
netcardconfig	Selectați acest tip de conexiune dacă folosiți o rețea locală (LAN) pentru acces la Internet. A se folosi şi 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 ştiți 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 aceşti paşi:

1. Faceți clic-dreapta pe desktop. Va apărea meniul contextual al BitDefender Rescue CD.
2. Selectați **Terminal (as root)**.
3. Introduceți următoarele comenzi:

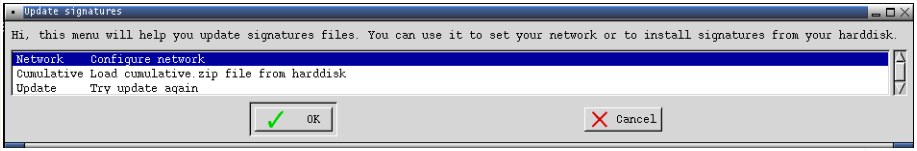
```
# pppconfig
```

4. Urmați instrucțiunile de pe ecran. Dacă nu ştiți ce să scrieți, contactați administratorul sistemului sau rețelei dumneavoastră pentru detalii.

30.5. Cum actualizez BitDefender?

La pornirea sistemului, se face automat actualizarea semnăturilor de viruşi. Dacă ați sărit acest pas, iată cum puteți actualiza BitDefender.

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 şi încărcând fişierul `cumulative.zip`.
   - Selectați **Update** pentru a vă conecta imediat la internet şi descărca ultimele semnături de viruşi.
3. Faceți clic pe **OK**.

30.5.1. Cum actualizez BitDefender peste un proxy?

Dacă există un server proxy între calculatorul dumneavoastră şi Internet, trebuie efectuate anumite configurări pentru a actualiza semnăturile de viruşi.

Pentru a actualiza BitDefender peste un proxy, urmați aceşti paşi:

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 fişier utilizând GNU Midnight Commander (mc).
5. Activați următoarea linie: `#HttpProxy =` (prin ştergerea simbolului #) şi specificați domeniul, numele de utilizator, parola şi portul serverului proxy. De exemplu, linia respectivă poate arăta astfel:

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```
6. Apăsați **F2** pentru a salva fişierul curent, confirmați salvarea şi apoi apăsați **F10** pentru a-l închide.
7. Introduceți comanda: **bdscan update**.

30.6. Cum îmi salvez datele?

Să presupunem că nu puteți porni calculatorul dumneavoastră, cu Windows instalat, din cauza unor probleme necunoscute. În acelaşi 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 aceşti paşi:

1. Introduceți CD-ul cu BitDefender Rescue CD în unitatea CD-ROM, stickul de memorie în USB şi apoi reporniți calculatorul.

   Notă
   Dacă introduceți stickul de memorie mai târziu, va trebui să montați dispozitivul amovibil urmând aceşti paşi:
   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. Aşteptați până ce BitDefender Rescue CD porneşte calculatorul. Va apărea următoarea fereastră:

Ecran desktop

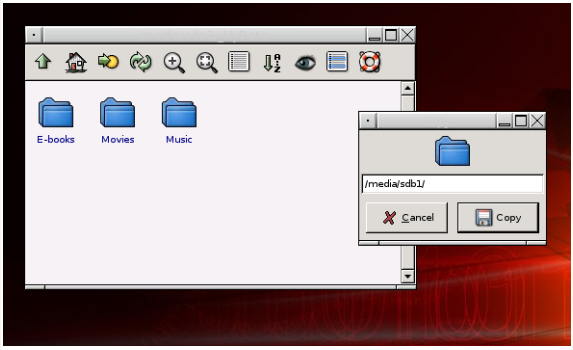
3. Faceți dublu-clic pe partiția unde se află datele pe care vreți să le salvați (de exemplu, `[sda3]`).

Notă
Atunci când lucrați cu BitDefender Rescue CD, veți avea de-a face cu nume de partiții de tip Linux. Aşadar, `[sda1]` va corespunde probabil partiției `(C:)` din Windows, `[sda3]` partiției `(F:)` şi `[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 aceşti paşi:
a. Faceți dublu-clic pe iconița Terminal Emulator de pe desktop.
b. Introduceți următoarea comandă:

```
# mount  /media/partition_name
```

4. Căutați printre directoare şi alegeți-l pe cel dorit. De exemplu, `MyData` care conține subdirectoarele `Movies`, `Music` şi `E-books`.
5. Faceți clic-dreapta pe directorul dorit şi selectați **Copiază**. Va apărea următoarea fereastră.



Salvarea datelor

6. Introduceți `/media/sdb1/` în căsuța de text corespunzătoare şi faceți clic pe **Copiază**.

   Vă rugăm să țineți cont că în funcție de configurația calculatorului dumneavoastră, acesta poate fi `sda1` în loc de `sdb1`.

Vocabular

ActiveX

ActiveX este un mod de scriere a programelor astfel încât să poată fi apelate de celelalte programe şi sisteme de operare. Tehnologia ActiveX este utilizată pentru realizarea de pagini Web interactive care se comportă ca nişte aplicaţii şi nu ca nişte simple pagini statice. Cu elemente de ActiveX, utilizatorii pot răspunde la întrebări, să utilizeze butoane şi să interacţioneze şi 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 securităţii; experţii în securitatea calculatoarelor descurajează utilizarea lui pe Internet.

Adware

Aplicaţia adware este adesea combinată cu o aplicaţie gazdă care este oferită gratuit dacă utilizatorul acceptă aplicaţia adware. Deoarece aplicaţiile adware sunt de obicei instalate după ce utilizatorul a fost de acord în prealabil cu un contract de licenţiere care explică scopul aplicaţiei, nu este comisă nicio infracţiune.

Totuşi, reclamele de tip pop-up pot fi supărătoare, iar în unele cazuri pot afecta performanţele sistemului. De asemenea, informaţiile pe care unele dintre aceste aplicaţii le adună pot cauza motive de îngrijorare utilizatorilor care nu cunosc în întregime termenii din contractul de licenţiere.

Arhivă

Un disc, o casetă sau un director care conţine fişiere de rezervă.

Un fişier care conţine unul sau mai multe fişiere într-un format comprimat.

Backdoor

Reprezintă o gaură de securitate realizată în mod deliberat. Motivaţia acestor "găuri" nu este întotdeauna maliţioasă: unele sisteme de operare, de exemplu, sunt puse în circulaţie cu conturi privilegiate pentru tehnicienii din service sau de responsabilii cu mentenanţă produsului din partea vânzătorului.

Sector de boot

Un sector la începutul fiecărui disc care identifică arhitectura discului (mărimea sectorului, mărimea clusterului şi altele). În cazul discurilor de startup, sectorul de boot conţine 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 şi încărca pagini de Web. Două din cele mai populare browsere sunt Mozilla Firefox şi Microsoft Internet Explorer. Ambele sunt browsere grafice, ceea ce înseamnă că pot afişa atât grafice cât şi text. În plus, cele mai moderne browsere pot prezenta informații multimedia, incluzând sunet şi 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 şi care este actualizat de fiecare dată când utilizatorul accesează din nou site-ul. Serverul, la fel ca şi browserul, salvează informațiile despre utilizator conținute în cookie. Aceste informații sunt stocate sub forma unui fişier text în directoarele de sistem ale browserelor Netscape şi Explorer;nu toate browserele suportă cookie. Fişierele cookie stochează informații cum ar fi numele utilizatorului şi parola, cât şi 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 fişiere cookie sunt programate cu dată de expirare, astfel încât ele vor fi şterse automat după o anumită perioadă de timp.

Drive de disc

Este un dispozitiv care citeşte date de pe un disc şi scrie date pe un disc.

Un drive de hard disc citeşte / 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).

Download

Reprezintă copierea (de obicei a unui întreg fişier) de pe o sursă principală pe un dispozitiv periferic. Termenul este adesea utilizat pentru a descrie procesul de copiere a unui fişier de pe un serviciu on-line pe calculatorul unui utilizator. De asemenea se mai poate referi şi la copierea unui fişier de pe un server de rețea pe un calculator din rețea.

E-mail

Se referă la poşta electronică. Acesta este un serviciu care transmite mesaje prin intermediul reţelei locale sau globale.

Evenimente

O acţiune sau întâmplare detectată de un program. Evenimentele pot fi acţiuni 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 fişier ca fiind infectat când de fapt acesta nu este infectat.

Extensie de fişier

Reprezintă porţiunea dintr-un nume de fişier ce urmează după caracterul punct, şi care indică tipul de date pe care le stochează fişierul.

Multe sisteme de operare, cum ar fi Unix, VMS, and MS-DOS, utilizează extensii de fişiere. 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 fişierele text oarecare, "c" pentru fişierele sursă scrise în limbajul C, etc.

Metoda euristică

Reprezintă o metodă bazată pe anumite reguli pentru identificarea de viruşi noi. Această metodă de scanare nu se bazează pe semnături de viruşi cunoscuţi. Avantajul metodei euristice e dat de faptul că nu poate fi păcălită de o nouă variantă a unui virus deja existent. Totuşi ocazional poate raporta un cod suspicios în programe normale, generând aşa-numitul "fals pozitiv".

IP

Internet Protocol - Un protocol rutabil din suita protocoalelor TCP / IP căruia i se atribuie adresarea IP, rutarea, fragmentarea cât şi 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 şi mărimea acestuia. Când este accesată o pagină web, browser-ul descarcă applet-ul de pe un server şi îl rulează pe maşina utilizatorului (clientul). Applet-urile diferă de aplicaţii prin aceea că sunt guvernate de un protocol de securitate strict.

Astfel că, deşi pot rula pe calculatorul unui utilizator, ele nu pot citi sau scrie date pe aceste calculatoare. Applet-urile sunt restricţionate de domeniul de care aparţin în ceea ce priveşte scrierea şi 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 şi Excel suportă limbaje macro puternice.

Aceste limbaje permit încapsularea de macro-uri în documente şi 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 şi să recepționați mesaje.

Memorie

Reprezintă arii de stocare a datelor din interiorul calculatorului. Termenul de memorie desemnează locul de stocare a datelor pe chipuri şi 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 viruşi. Avantajul metodelor ne-euristice constă în aceea că scannerul nu poate fi "păcălit" de ceea ce poate părea un virus şi din acest motiv nu generează fals pozitiv.

Programe împachetate

Reprezintă un fişier în format comprimat. Multe din sistemele de operare şi aplicații conțin comenzi care vă dau posibilitatea de a împacheta un fişier astfel încât să ocupe mai putină memorie. De exemplu, să presupunem că aveți un fişier text care conține zece caractere reprezentând spații. În mod normal, acesta ar necesita zece biți de memorie pentru a fi stocați.

Totuşi, un program care împachetează fişiere 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 fişier de pe un calculator. Această direcție este specificată utilizând sistemul ierarhic de organizare a fişierelor 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 şi numere de card de credit, de asigurări sociale şi de conturi bancare pe care compania respectivă deja le are. Site-ul Web este însă fals şi folosit pentru a fura informațiile despre utilizator.

Virus polimorf

Reprezintă un virus care îşi schimbă forma cu fiecare fişier pe care îl infectează. Din cauză că nu au un tipar binar consistent, asemenea viruşi 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 şi tastaturilor. Există porturi externe pentru conectarea modemului, imprimantei, mouse-ului şi a altor dispozitive periferice.

În rețelele TCP / IP şi 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.

Fişier de raport

Reprezintă un fişier care listează acțiunile care au avut loc. BitDefender menține un fişier log (jurnal) în care sunt listate obiectele care au fost scanate, numele fişierelor, numărul de arhive şi fişiere scanate, câte fişiere infectate şi 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 şi se referea la unelte recompilate ce furnizau intruşilor drepturi administrative, permițându-le să îşi ascundă prezența astfel încât să nu poată fi văzuți de către administratorii de sistem.

Rolul principal al rootkiturilor este de a ascunde procese, fişiere, loginuri şi 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 şi chiar unele aplicații ascunde fişiere critice utilizând rootkituri. Totuşi, ele sunt folosite în general

pentru a ascunde aplicații malițioase sau prezența intruşilor în sistem. În combinație cu aplicații malițioase, rootkiturile constituie o mare amenințare pentru securitatea şi integritatea sistemului. Acestea pot monitoriza traficul, crea porți de acces în sistem ("backdoors"), altera fişiere şi jurnale şi evita detecția.

Script

Un alt termen pentru fişiere 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 ştirea 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; totuşi, trebuie ştiut că majoritatea aplicațiilor de tip shareware şi freeware nu conțin aplicații spyware. Odată instalată, aplicația spyware monitorizează activitatea utilizatorului pe Internet şi transmite pe ascuns informații altei persoane. Aplicațiile spyware pot aduna, de asemenea, informații despre adresele e-mail şi chiar parole şi numere de carduri de credit.

Asemănarea dintre spyware şi un cal troian este faptul că utilizatorul instalează aplicația fără voia sa atunci când instalează altceva. Un mod obişnuit de a deveni victima unei aplicații spyware este de a descărca prin rețelele peer-to-peer anumite produse de schimb de fişiere care sunt disponibile astăzi.

Pe lângă problemele legate de etică şi intimitate, aplicația spyware fură de la utilizator atât prin folosirea memoriei calculatorului cât şi a lungimii de bandă deoarece trimite informații înapoi la sursă prin intermediul conexiunii la Internet a utilizatorului. Deoarece folosesc memorie şi resurse ale sistemului, aplicațiile spyware pot conduce la blocarea sistemului sau la instabilitate generală.

Elemente din startup

Orice fişier 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, şi nu direct fişierul.

Bara de sistem

Introdusă odată cu apariția sistemului Windows 95, bara de sistem este plasată în taskbar-ul de Windows (situat lângă ceas) şi conține iconițe pentru accesul rapid la aplicații sistem cum ar fi cele legate de fax, imprimantă, modem, volum,

şi altele. Executați dublu-clic cu mouse-ul pe o iconiță pentru a vizualiza şi accesa elementele.

TCP/IP

Transmission Control Protocol/Internet Protocol - Un set de protocoale de rețea folosite în mod larg în domeniul Internet şi care asigură comunicarea între rețelele de calculatoare interconectate având arhitecturi hardware şi sisteme de operare diferite. TCP/IP include standarde referitoare la realizarea comunicării între calculatoare cât şi convenții folosite în conectarea rețelelor şi rutării traficului.

Troian

Este un program distructiv care este mascat sub forma unei aplicații benigne. Spre deosebire de viruşi, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cei mai mascați troieni este acela care pretinde că elimină viruşii de pe computerul dumneavoastră, dar în loc de aceasta, introduce viruşi pe calculatorul dumneavoastră.

Termenul provine de la o poveste din opera "Iliada" lui Homer, în care grecii oferă duşmanilor lor, troienii, în semn de pace un cal gigantic de lemn. Dar după ce troienii aduc acest cal în interiorul oraşului lor, din interiorul calului ies o mulțime de soldați greci, care deschid porțile cetății, permițându-le celorlalți soldați greci să pătrundă în oraş şi să captureze Troia.

Actualizare

O versiune nouă de produs hardware sau software proiectat să înlocuiască o versiune mai veche a aceluiaşi 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 ştirea dumneavoastră şi rulează independent de voința dumneavoastră. Cea mai mare parte a viruşilor se pot şi înmulți. Toți viruşii informatici sunt creați de om. Un simplu virus care poate realiza copii ale sale este relativ simplu de produs. Chiar şi un asemenea virus este periculos întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. Un virus şi mai periculos este acela care este capabil să se răspândească în rețea şi poate să treacă de sistemele de securitate.

Semnătură de virus

Reprezintă tiparul binar al unui virus, utilizat de un program antivirus pentru detecția şi eliminarea virusului.

Vierme

Reprezintă un program care se autopropagă în interiorul unei rețele, reproducându-se pe măsură ce se răspândeşte. Nu se poate ataşa la alte programe.