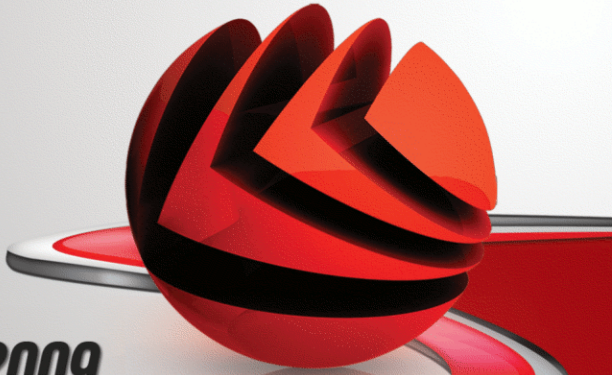
bitdefender



ANTIVIRUS 2009

Manual de utilizare

bitdefender

BitDefender Antivirus 2009

Manual de utilizare

Publicat 2008.08.26

Termeni legali

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 deținеți 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 Antivirus 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 Antivirus 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 Antivirus 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. xiii)	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 Antivirus 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 malițioase (viruşi, aplicații spyware, rootkit-uri 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 Antivirus 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)
- 170 MB spațiu disponibil pe hard disc (200 MB recomandat)

Pentru Windows Vista

- Procesor de 800 MHz sau superior
- 512 MB memorie RAM (1 GB recomandat)
- 170 MB spațiu disponibil pe hard disc (200 MB recomandat)

Pentru Windows Home Server

- Procesor de 800 MHz sau superior
- 512 MB memorie RAM (1 GB recomandat)
- 170 MB spațiu disponibil pe hard disc (200 MB recomandat)

1.2. Cerințe software

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

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

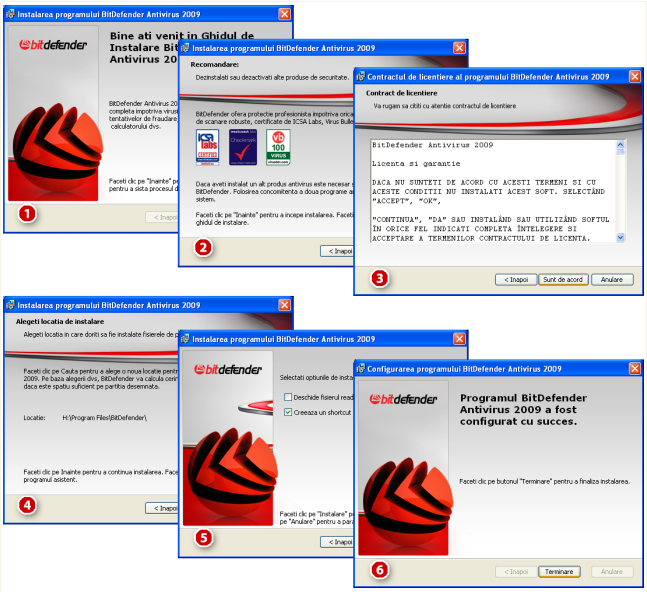
Criptarea mesageriei instant (IM) este oferită doar pentru:

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

2. Instalarea BitDefender

Localizați fişierul 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 fişierului 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 fişierul de instalare.



Etapele instalării

Urmați aceşti paşi pentru a instala BitDefender Antivirus 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 Antivirus 2009 vă alertează dacă aveți un alt produs antivirus instalat 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 Antivirus 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 o scurtătură (shortcut) către BitDefender Antivirus 2009 pe desktop la sfârşitul 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 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 Antivirus 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

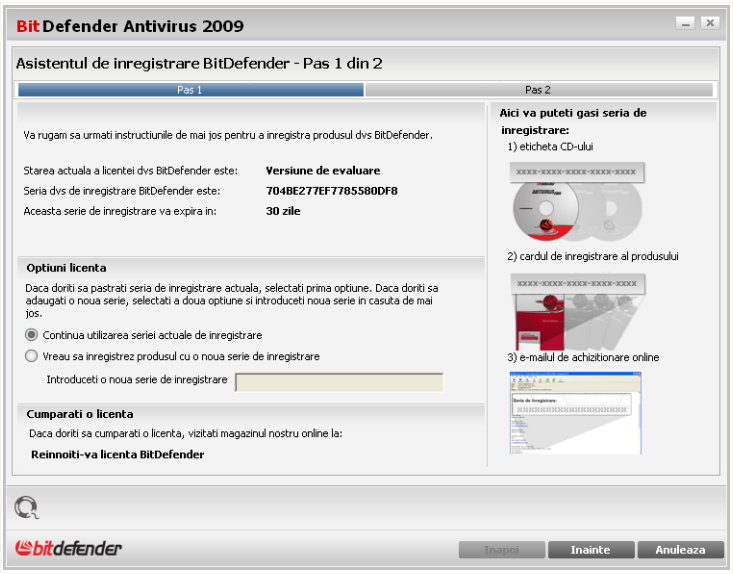
Prima dată când porniți calculatorul după instalare, va apărea un program asistent de înregistrare. Programul asistent vă ajută să înregistrați BitDefender şi să configurați un cont BitDefender.

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 Antivirus 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 Antivirus 2009:

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

Notă

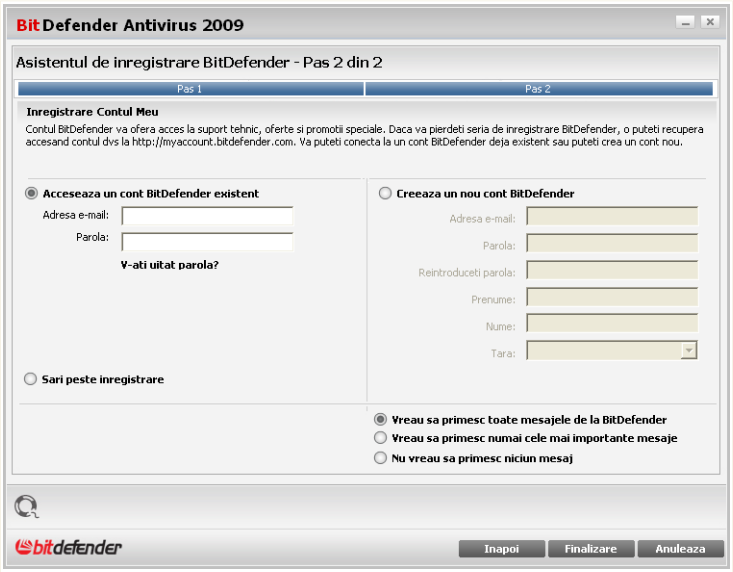
Puteți găsi seria dumneavoastră de înregistrare:

- 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 Antivirus 2009.

Notã

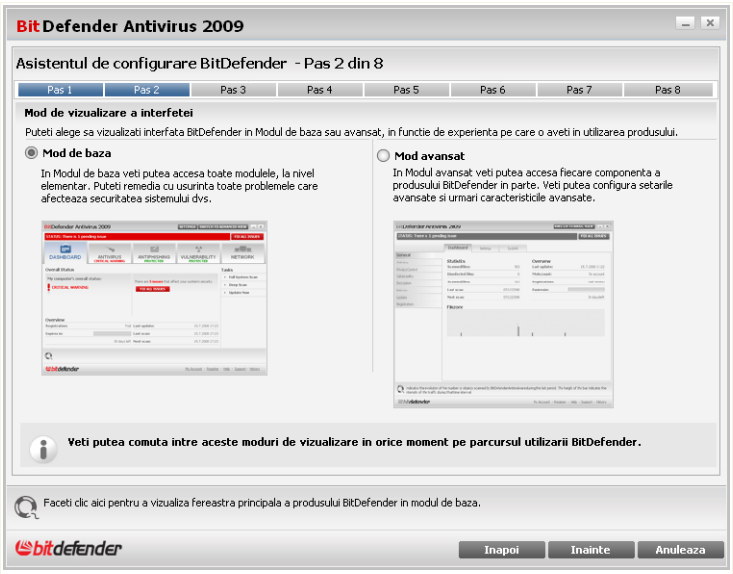
Dacă nu doriți să urmați acest program asistent, faceți clic pe **Anulare**. BitDefender vă va informa despre componentele care trebuie configurate atunci când deschideți fereastra principală a produsului.

2.2.1. Pasul 1/8 - Fereastra de întâmpinare

Fereastra de întâmpinare

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

2.2.2. Pasul 2/8 - Selectați modul de vizualizare



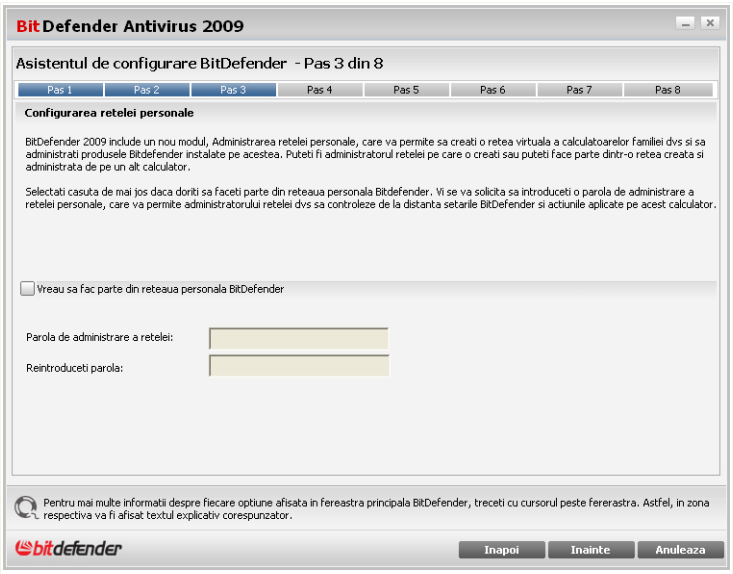
Moduri de vizualizare

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 3/8 - 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:

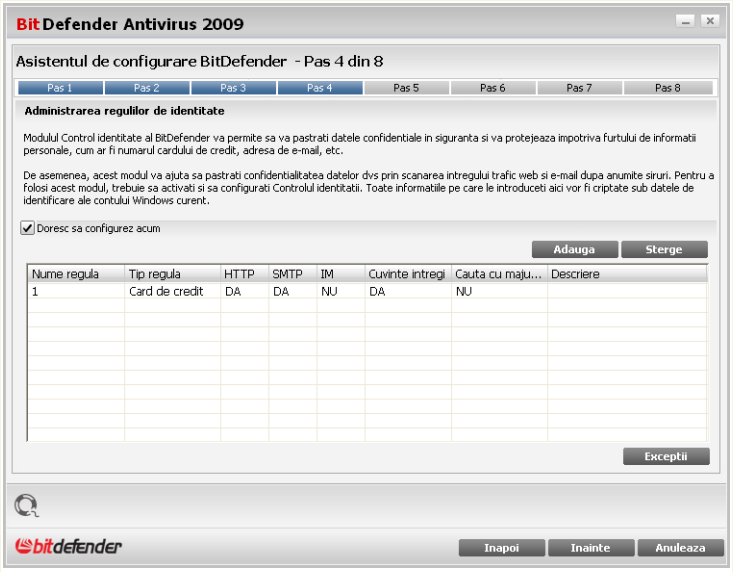
1. Selectați **Vreau să fac parte din rețeaua personală BitDefender**.
2. Introduceți aceeaşi parolă administrativă în fiecare dintre câmpurile editabile.

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 4/8 - 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.

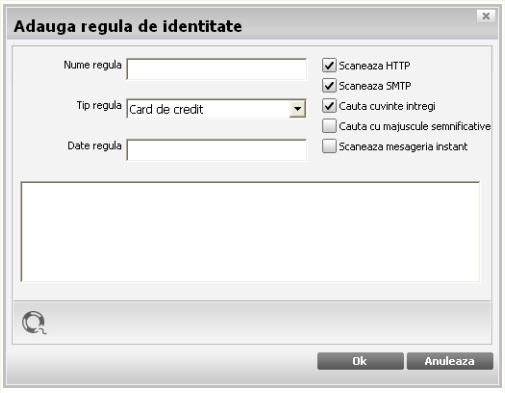
Dacă doriți să utilizați Controlul identității, urmați aceşti paşi:

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:

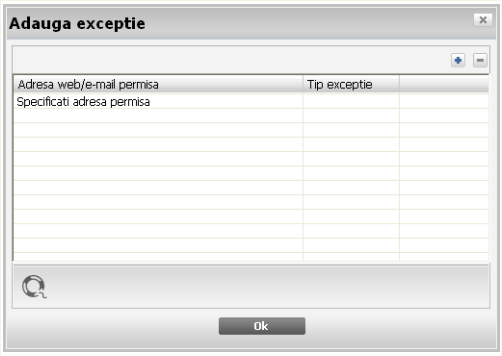
- **Scanează HTTP** - scanează traficul HTTP (web) şi blochează la ieşire toate datele care corespund unei reguli.
- **Scanează SMTP** - scanează traficul SMTP (mail) şi blochează trimiterea mesajelor e-mail care corespund unei reguli.
- **Scanează mesageria instant** - scanează traficul de mesagerie 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 5/8 - 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.

2.2.6. Pasul 6/8 - Selectați sarcinile ce vor fi rulate

Selectare sarcini

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

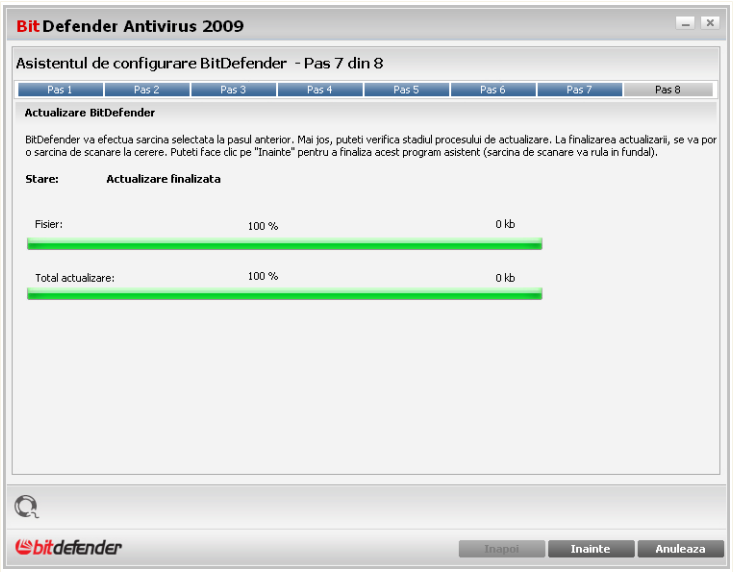
- **Actualizează motoarele BitDefender (poate fi necesară repornirea sistemului)** - în timpul pasului următor va fi efectuată o actualizare a motoarelor BitDefender pentru a vă proteja sistemul împotriva celor mai noi amenințări.
- **Rulează o scanare rapidă a sistemului (poate fi necesară repornirea 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.

2.2.7. Pasul 7/8 - 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.

2.2.8. Pasul 8/8 - 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 Antivirus 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 Antivirus 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
  Doar pentru Windows Vista! Dezinstalând BitDefender, nu veți mai fi protejat împotriva amenințărilor malițioase, precum viruşii şi aplicațiile spyware. Dacă doriți activarea Windows Defender după dezinstalarea BitDefender, selectați căsuța corespunzătoare.

  Faceți clic pe **Dezinstalare** pentru a iniția ştergerea completă a BitDefender Antivirus 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 Antivirus 2009

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

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

4.2. Modul de vizualizarea a interfeței cu utilizatorul

BitDefender Antivirus 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.
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.

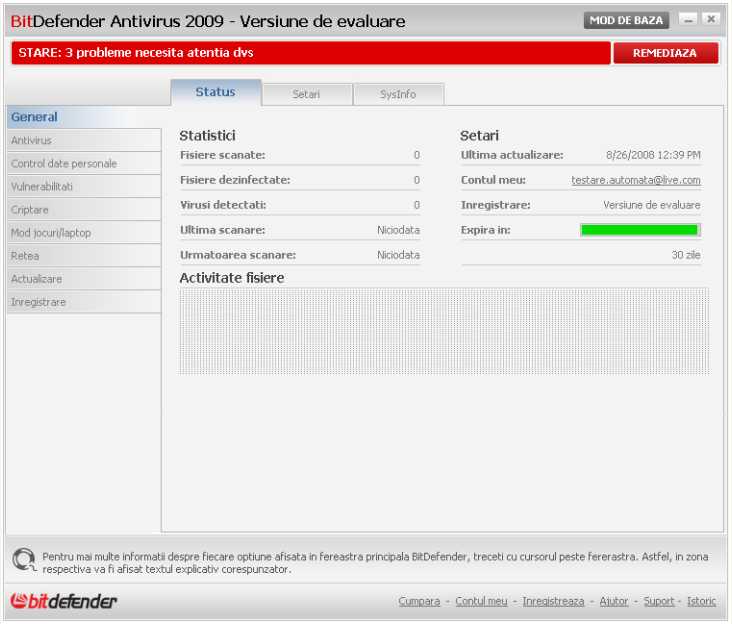
Tab	Descriere
Sumar	Afişează statistici importante despre produs şi statusul înregistrării, împreună cu linkuri către cele mai importante sarcini la cerere.
Antivirus	Afişează starea modulului antivirus care vă ajută să actualizaţi BitDefender şi să vă protejaţi sistemul de viruşi.
Antiphishing	Afişează starea modulului antiphishing care vă asigură că toate paginile web accesate de către dumneavoastră prin intermediul Internet Explorer sau Firefox sunt sigure.
Vulnerabilitate	Afişează starea modulului vulnerabilitate care vă ajută să menţineţi actualizate cele mai importante aplicaţii de pe calculatorul dumneavoastră.
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. Puteţi 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.
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.
Control date	Vă permite să preveniți furtul de date de pe calculatorul dumneavoastră şi să vă protejați confidențialitatea în timp ce sunteți online.
Criptare	Vă permite să criptați comunicațiile prin Yahoo şi Windows Live (MSN) Messenger.
Vulnerabilitate	Vă permite să mențineți actualizate cele mai importante aplicații de pe calculatorul dumneavoastră.
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 Antivirus 2009, să schimbați seria de înregistrare sau să creați un cont BitDefender.

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

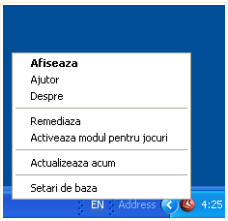
Link	Descriere
Contul meu	Vă permite să creați sau să vă conectați la contul dumneavoastră BitDefender. Contul BitDefender vă oferă acces gratuit la suport tehnic.

Link	Descriere
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 Antivirus 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.

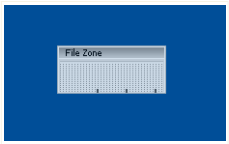
Dacă există probleme critice care afectează securitatea sistemului dumneavoastră, un semn de exclamare este afişat pe iconița BitDefender. Puteți ține cursorul

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.



Bara de scanare

Notă
Bara de scanare vă va avertiza când protecția în timp real este dezactivată prin afişarea unui X roşu deasupra zonei **Fişiere**.

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. 130).

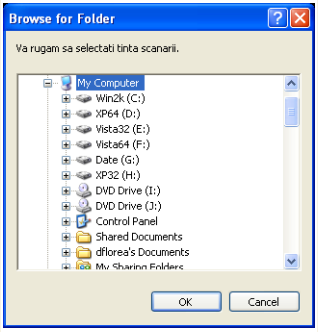
Când nu mai doriți să vedeți reprezentarea grafică, faceți doar clic-dreapta pe ea şi selectați **Închide**. Pentru a ascunde permanent această fereastră, urmați aceşti paşi:

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 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.

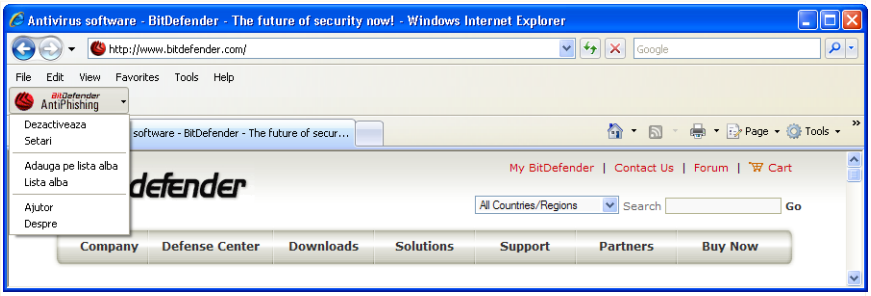
BitDefender se integrează direct, printr-o bară de comenzi intuitivă şi uşor de folosit, cu următoarele browsere web:

- 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.

4.8. 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.

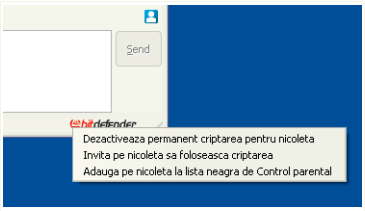
Important

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

5.1. 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.

Element	Descriere
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.

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 Antivirus 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**.

5.2. 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).
- **Actualizează acum** - inițiază o actualizare imediată.

5.2.1. 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.

Notă

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

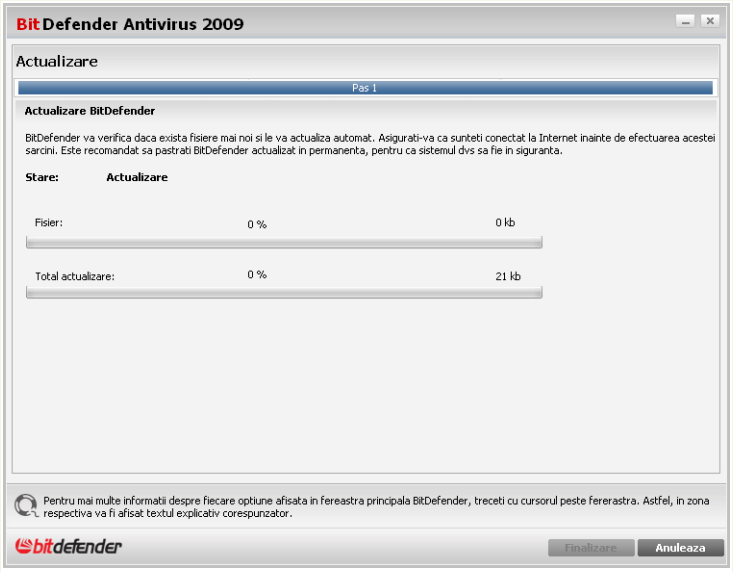
Atunci când iniţiaţi un proces de scanare la cerere, fie o scanare rapidă sau completă a sistemului, va apărea programul asistent de scanare.

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

5.2.2. Actualizarea BitDefender

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

În mod implicit, BitDefender caută actualizări atunci când deschideţi calculatorul şi apoi **la fiecare oră**. Cu toate acestea, dacă doriţi să actualizaţi BitDefender, trebuie doar să faceţi clic pe **Actualizează acum**. Procesul de actualizare va fi iniţiat 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.

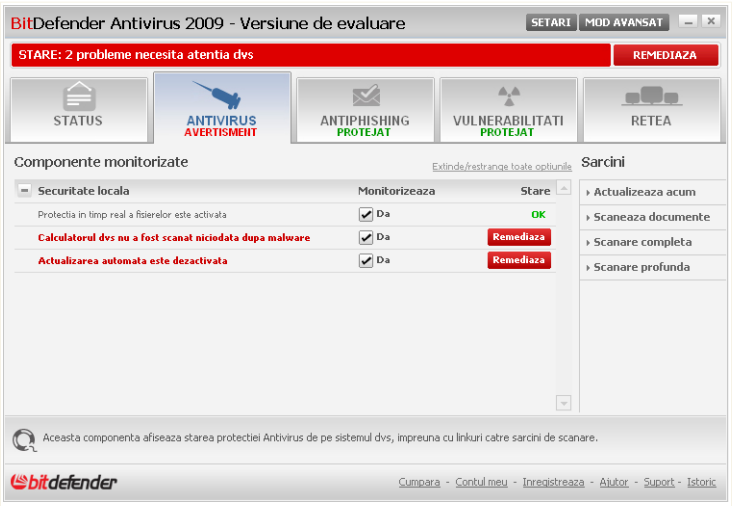
Faceți clic pe **Reboot** pentru a vă reporni imediat sistemul.

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

6. Antivirus

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

Pentru a accesa modulul Antivirus, faceți clic pe tabul **Antivirus**.



Antivirus

Modulul Antivirus 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

Componenta monitorizată este următoarea:

Categorie	Descriere
Securitate locală	Aici puteți verifica starea fiecărui modul de securitate care protejează obiectele stocate pe calculatorul dumneavoastră (fişiere, regiştri, memorie, etc.)

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 Antivirus 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**.

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.
- **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

Sarcina	Descriere
	ar fi viruşii, aplicaţiile spyware, aplicaţiile adware, aplicaţiile ascunse (rootkituri) şi altele.
Scanează Documentele mele	Utilizaţi această sarcină pentru a scana directoare importante ale utilizatorului curent: `My Documents`, `Desktop` şi `StartUp`. Astfel, veţi asigura siguranţa documentelor dumneavostră, un spaţiu de lucru sigur şi rularea la pornirea sistemului a unor aplicaţii necompromise.
Scanare personalizată	Utilizaţi 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 rulaţi aceste sarcini cu prioritate scăzută sau, şi mai bine, atunci când nu utilizaţi calculatorul.

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

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

Scanare personalizată

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

Pasul 1/4 - Fereastra de întâmpinare

Aceasta este doar o pagină de bun venit.

Fereastra de întâmpinare

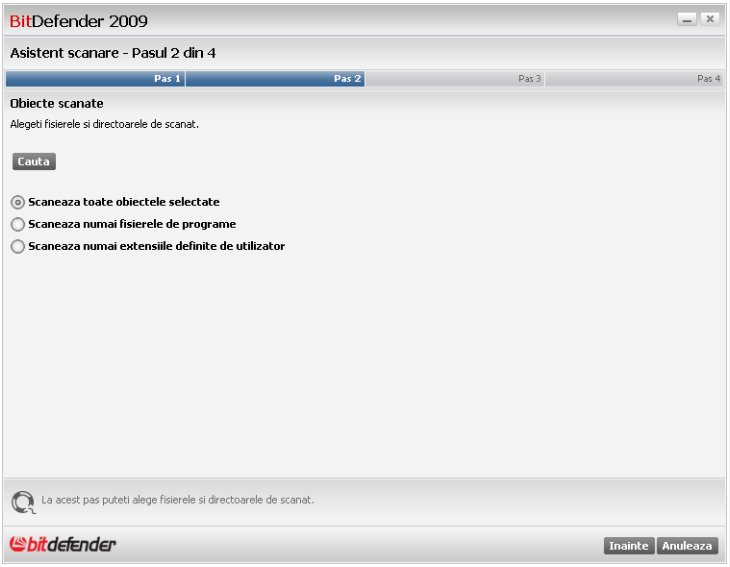
Cu ajutorul acestui program asistent vă veți putea scana calculatorul pentru a identifica eventualele pericole. Veți putea selecta anumite directoare şi/sau fişiere de scanat si veți putea stabili acțiuni de aplicat la detectarea unor fişiere infectate. De asemenea, veți primi un raport de scanare care 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.

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

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

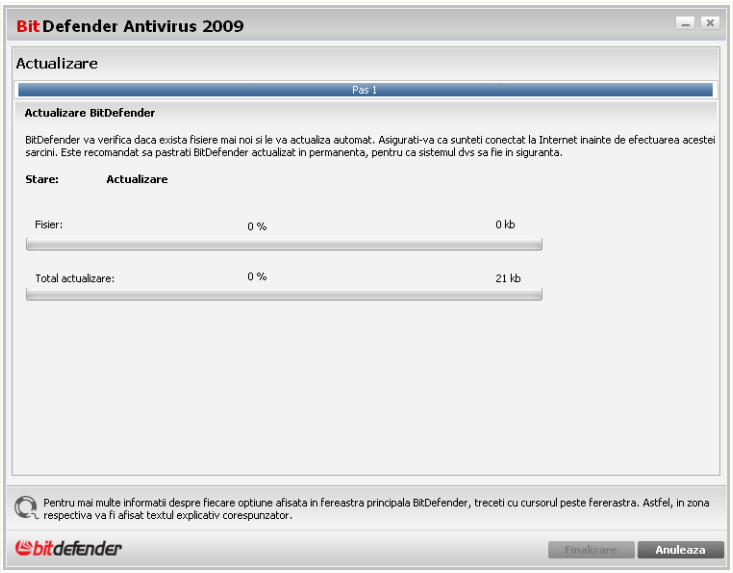
Faceți clic pe **Scanează** şi urmați programul asistent în trei paşi pentru a realiza procesul de scanare.

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.

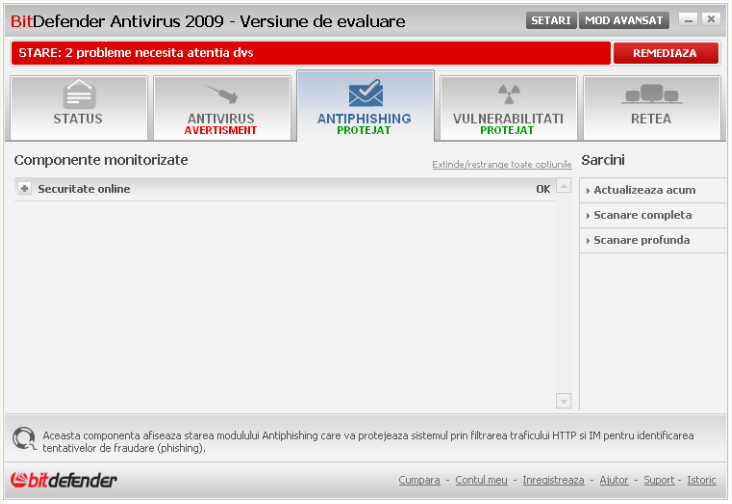
Faceți clic pe **Reboot** pentru a vă reporni imediat sistemul.

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

7. Antiphishing

BitDefender include un modul Antiphishing care verifică dacă paginile web accesate de către dumneavoastră prin intermediul Internet Explorer sau Firefox sunt sigure.

Pentru a accesa modulul Antiphishing, faceți clic pe tabul **Antiphishing**.



Antiphishing

Modulul Antiphishing 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.

7.1. Componente monitorizate

Componenta monitorizată este următoarea:

Categorie	Descriere
Securitate online	Aici puteti verifica starea modulelor de securitate care vă protejează tranzacțiile online şi calculatorul când sunteți conectat la Internet.

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

7.1.1. 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
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**.

7.2. 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.
- **Scanare personalizată**

7.2.1. 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`,

Sarcina	Descriere
	`Desktop` şi `StartUp`. Astfel, veți asigura siguranța 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.

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

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

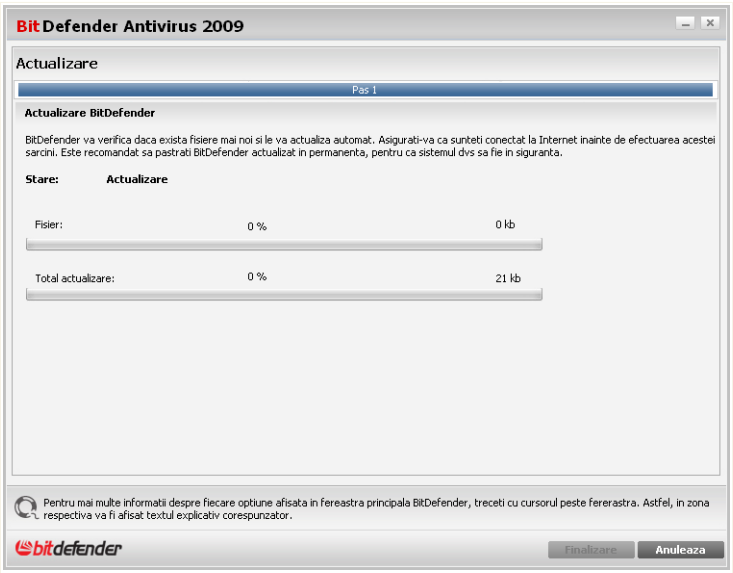
Faceți clic pe **Scanează** şi urmați programul asistent în trei paşi pentru a realiza procesul de scanare.

7.2.2. 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.

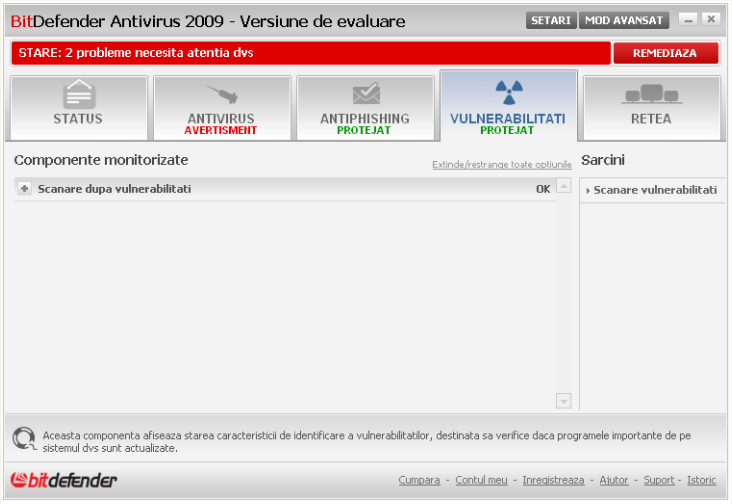
Faceți clic pe **Reboot** pentru a vă reporni imediat sistemul.

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

8. Vulnerabilitate

BitDefender include un modul Vulnerabilitate care vă ajută să mențineți actualizate aplicații critice de pe calculatorul dumneavoastră.

Pentru a accesa modulul Vulnerabilitate, faceți clic pe tabul **Vulnerabilitate**.



Vulnerabilitate

Modulul Vulnerabilitate 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 găsiți un link către o sarcină importantă de securitate.

8.1. Componente monitorizate

Componenta monitorizată este următoarea:

Categorie	Descriere
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.

8.1.1. 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**.

8.2. Sarcini

Aici găsiți un link către o sarcină importantă de securitate.

Următorul buton este disponibil:

- **Verificare vulnerabilități**

8.2.1. 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

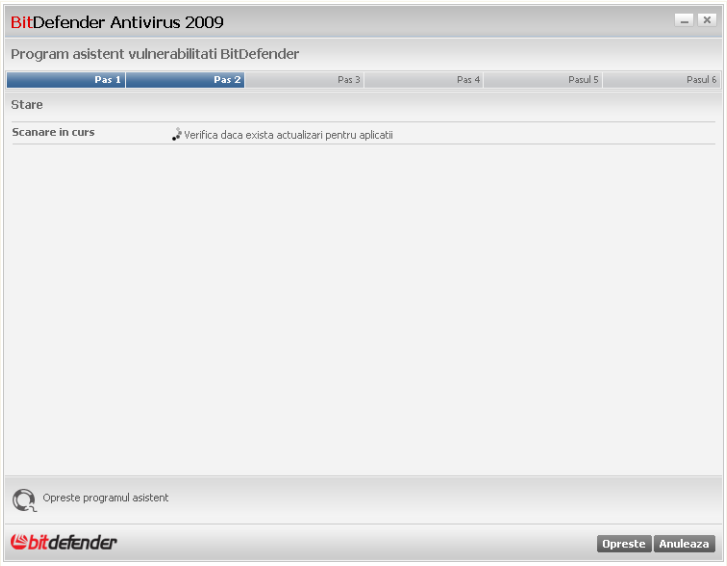
Pentru a verifica dacă sistemul dumneavoastră este vulnerabil, faceți clic pe **Verifică acum** şi urmați paşii programului asistent.

Pasul 1/6 - Selectați vulnerabilitățile de verificat

Vulnerabilități

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

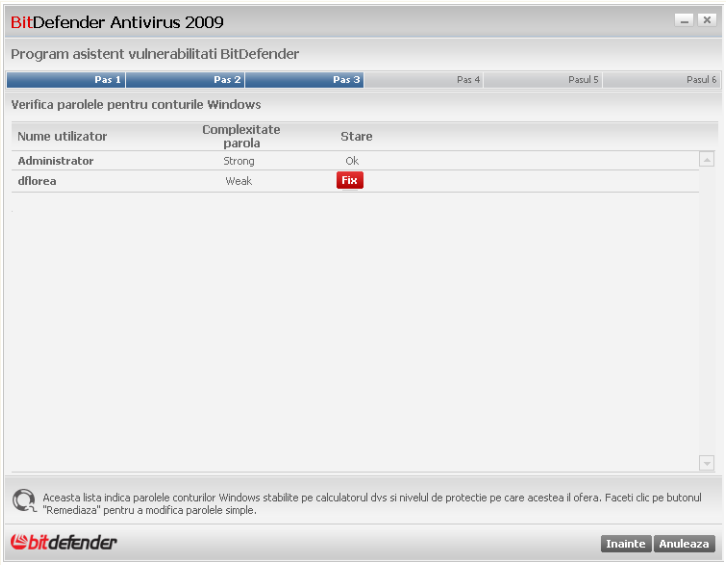
Pasul 2/6 - Căutare vulnerabilități



Căutare vulnerabilități

Aşteptați ca BitDefender să finalizeze căutarea.

Pasul 3/6 - Schimbaţi parolele slabe



Parole utilizatori

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

Faceţi 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.

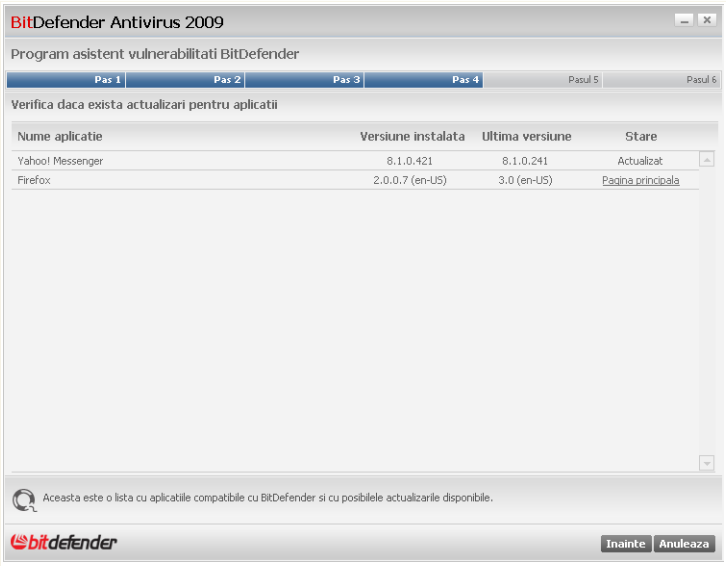
Notă

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

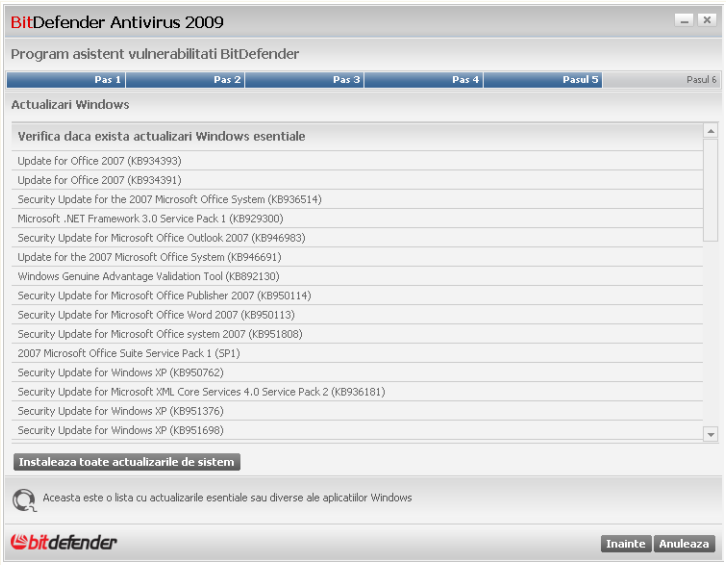


Aplicaţii

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

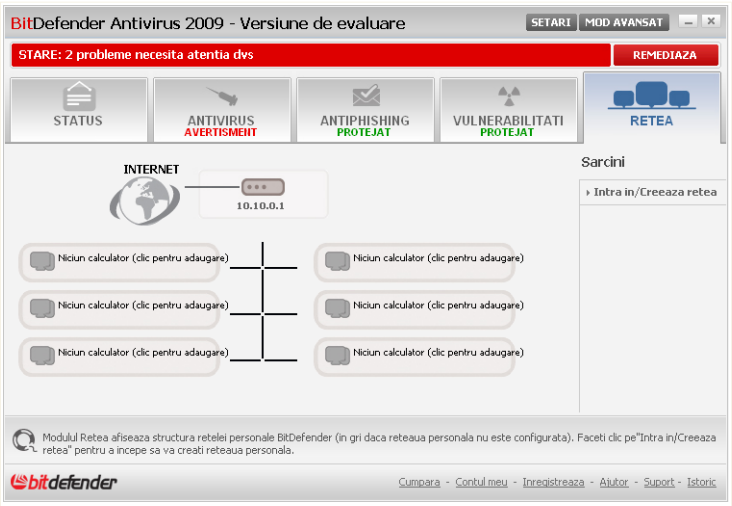
Rezultate

Faceți clic pe **Închide**.

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.

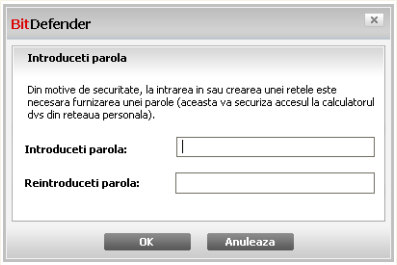
După intrarea în rețea, vor apărea mai multe butoane.

- **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**.

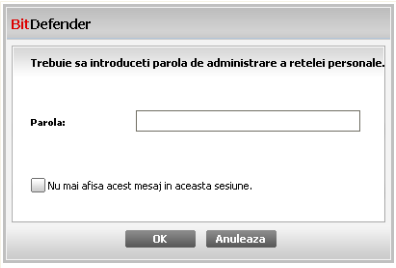
Puteți vedea numele calculatorului apărând pe harta rețelei.

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.

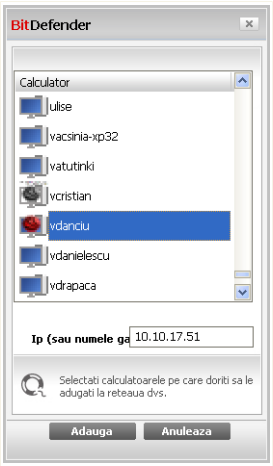
Pentru a adăuga un calculator la rețeaua BitDefender personală, urmați aceşti paşi:

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.

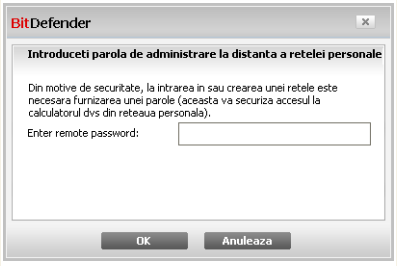


Adaugare calculator

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.



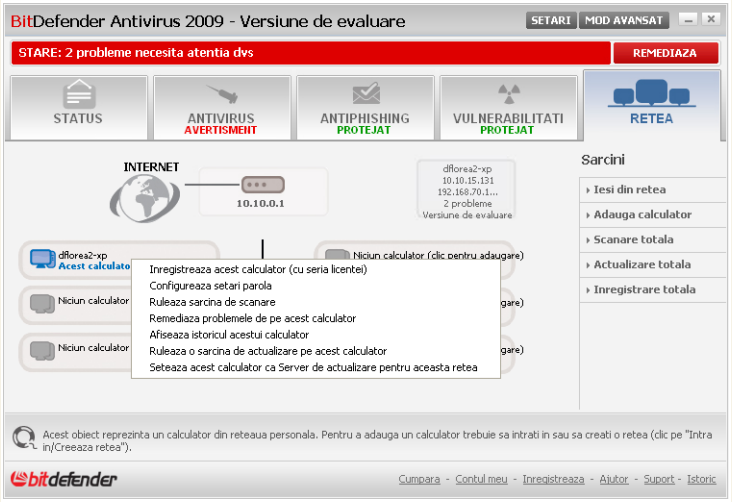
Autentificare

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.



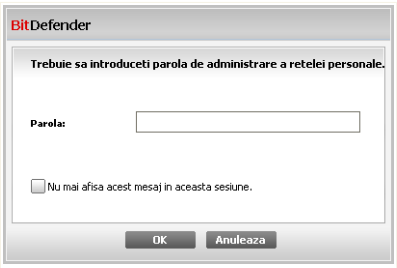
Hartă rețea

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**.

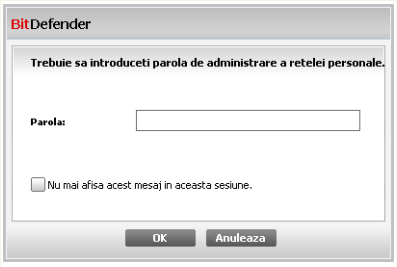
Notă

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

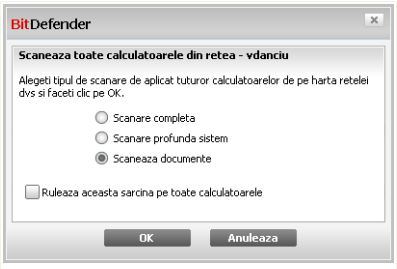
Pentru a scana toate calculatoarele administrate, urmați aceşti paşi:

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.



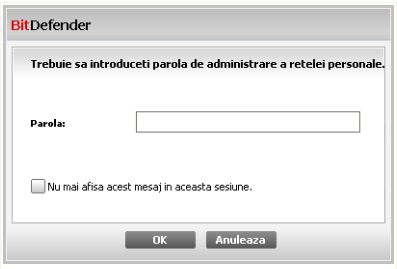
Selectați tipul de analiză.

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.



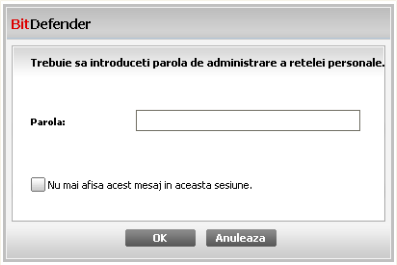
Introducere parolă

2. Faceți clic pe **OK**.

9.1.6. Înregistrarea tuturor calculatoarelor

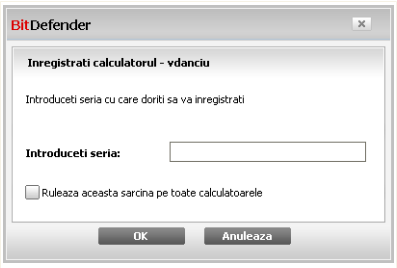
Pentru a înregistra toate calculatoarele administrate, urmați aceşti paşi:

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 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 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 generale

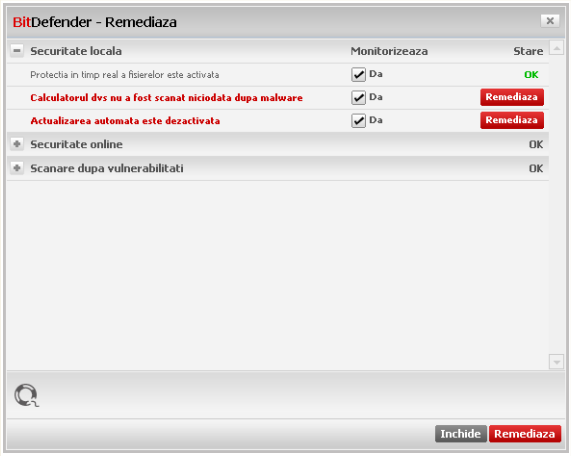
Puteți activa / dezactiva elemente legate de securitate cu un singur clic.

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.
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.
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 Antivirus 2009 există o bară de stare care afişează numărul de probleme existente. Faceţi clic pe butonul **Repară tot** pentru a elimina rapid orice ameninţări la adresa securităţii calculatorului dumneavoastră. Va apărea o fereastră care indică situaţia securităţii sistemului.

Fereastra afişează o listă organizată sistematic şi uşor de gestionat a vulnerabilităţilor de securitate de pe calculatorul dumneavoastră. BitDefender Antivirus 2009 vă va înştiinţa de fiecare dată când o problemă afectează securitatea calculatorului dumneavoastră.



Bara de stare

11.1. Securitate locală

Ştim că este important să fiţi înştiinţat ori de câte ori o problemă poate afecta securitatea calculatorului dumneavoastră. Prin monitorizarea fiecărui modul de securitate, BitDefender Antivirus 2009 vă va înştiinţa nu numai atunci când configuraţi setări care ar putea afecta securitatea calculatorului dumneavoastră, ci şi atunci când uitaţi să executaţi 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
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. 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.

Problemă	Descriere
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:

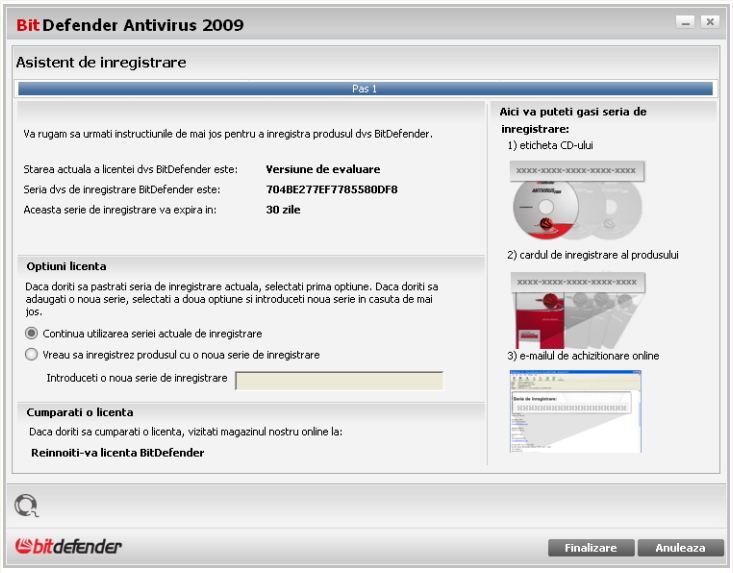
1. Faceți clic pe rând pe butoanele **Repară** pentru a remedia vulnerabilitățile sistemului dumneavoastră.
2. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

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

12. Înregistrare

Perioada de evaluare a BitDefender Antivirus 2009 este de 30 de zile. Dacă doriți să înregistrați BitDefender Antivirus 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 Antivirus 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 Antivirus 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:

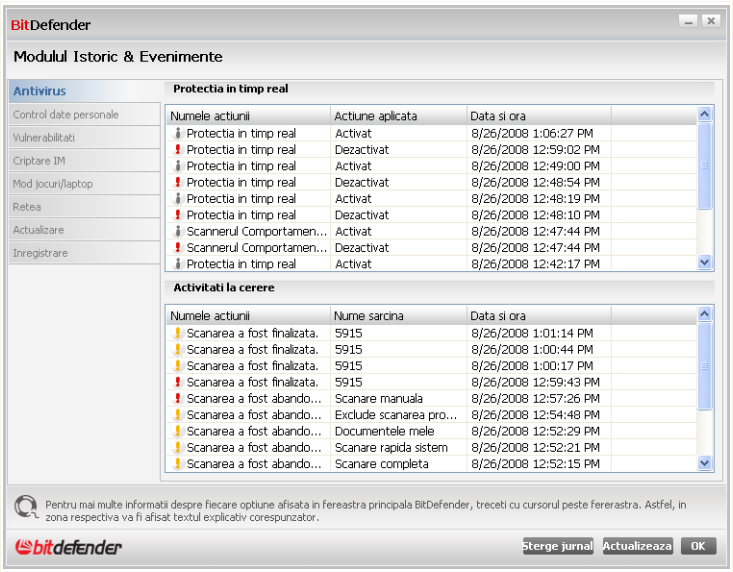
- pe eticheta de pe CD.
- pe certificatul de înregistrare al produsului.
- în e-mailul de achiziționare online.

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 etc.



Evenimente

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

- **Antivirus**
- **Control date**
- **Actualizare**
- **Rețea**

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.

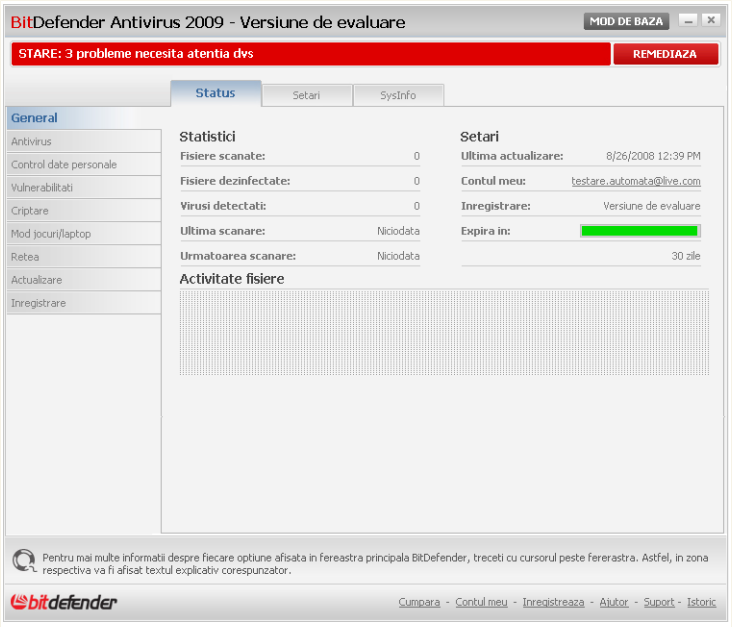
Administrare avansată

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.

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.

14.1.2. Descriere generală

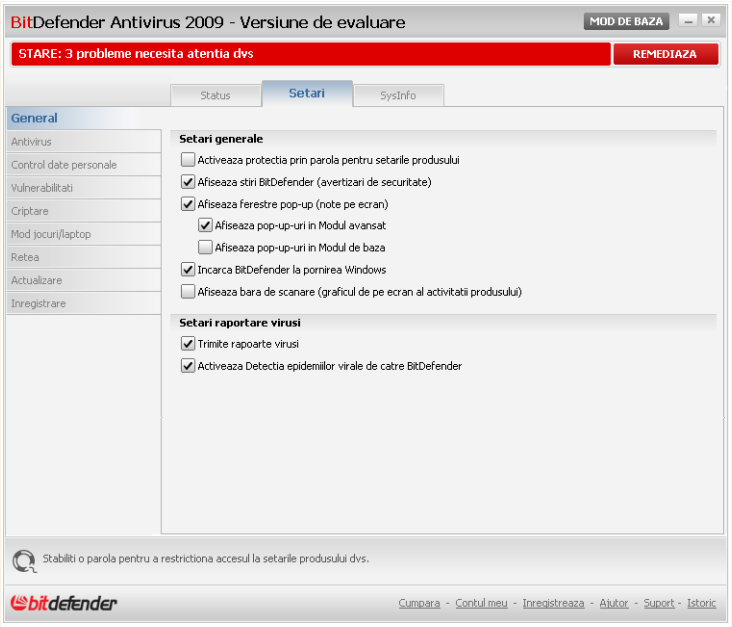
Aici puteti vedea un sumar al statisticilor cu privire la actualizare, contul dumneavoastră, înregistrare şi licenţă.

Element	Descriere
Ultima actualizare	Indică data la care produsul dumneavoastră BitDefender a fost actualizat ultima oară. Vă rugăm să efectuaţi actualizări în mod regulat, pentru a avea un sistem complet protejat.
Contul meu	Indică adresa de e-mail pe care o puteţi utiliza pentru a vă accesa contul online, unde vă puteţi recupera seria de înregistrare pierdută şi puteţi beneficia de suport BitDefender si alte servicii personalizate.
Înregistrare	Indică tipul şi starea seriei dumneavoastră de înregistrare. Pentru a menţine securitatea sistemului dumneavoastră, trebuie să reînnoiţi sau să actualizaţi versiunea BitDefender în cazul în care seria dumneavoastră a expirat.

Element	Descriere
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

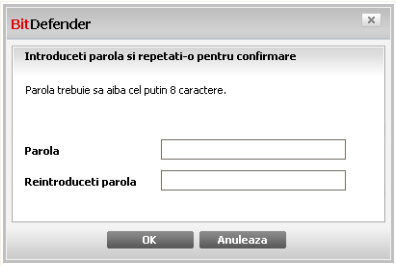
Aici puteți seta comportamentul general al produsului. BitDefender se încarcă la pornirea Windows iar apoi rulează minimizat în bara de sistem.

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.

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

- **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.

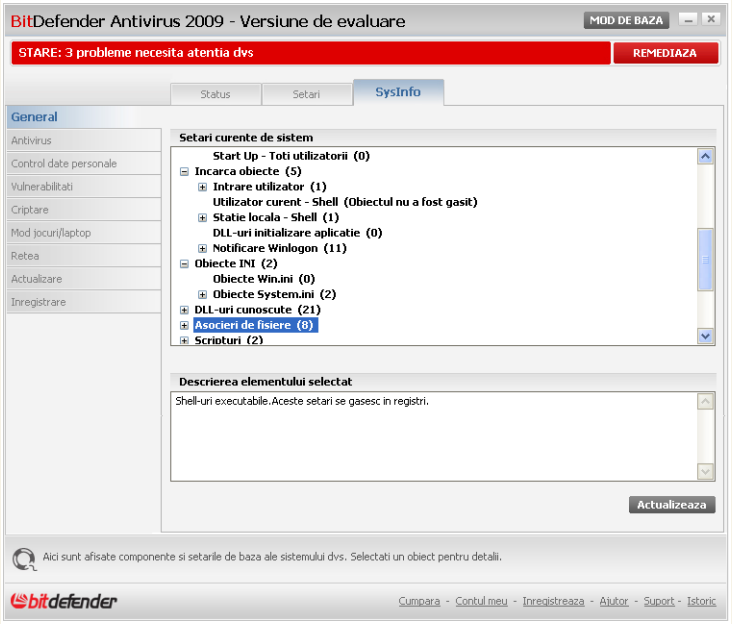
- **Activează Detecția epidemiilor virale de către BitDefender** - trimite Laboratorului BitDefender rapoarte referitoare la potențiale epidemii virale.

  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.

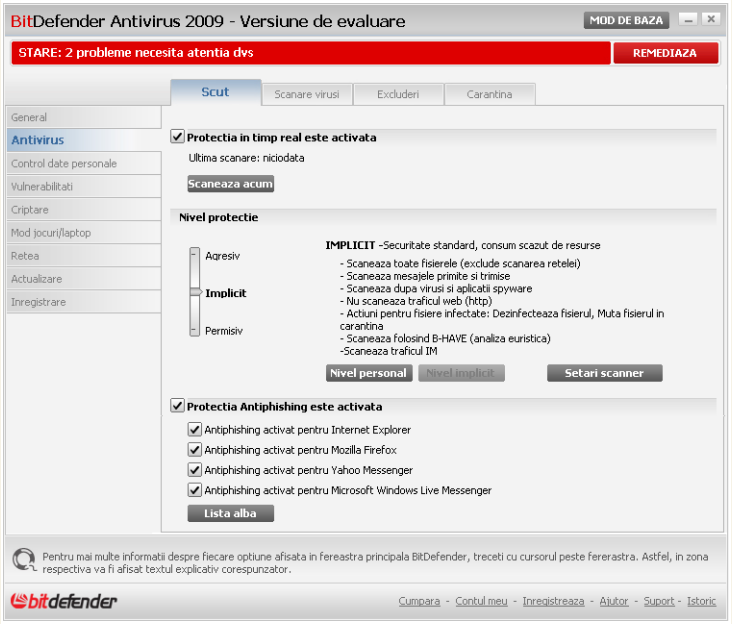
  Notă
  Protecţia în timp real mai este denumită şi scanare la acces - fişierele sunt scanate în timp ce utilizatorii le accesează.

- 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:

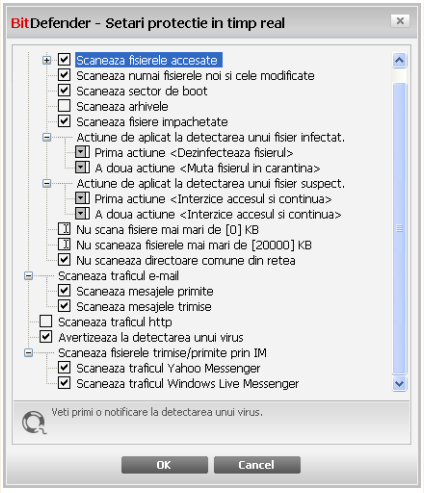
Nivel de protecţie	Descriere
Permisiv	Acoperă nevoile elementare de securitate. Consumul de resurse este foarte scăzut. Aplicaţiile şi mesajele e-mail primite sunt scanate doar împotriva viruşilor. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică. Acţiunile 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.

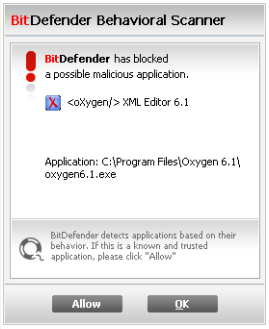
  Dacă este detectat un fişier suspect, din fereastra de alertă puteți lansa un program asistent ce vă va ajuta să trimiteți acest fişier Laboratorului BitDefender pentru analiză aprofundată. Pentru a primi informații despre acest fişier introduceți adresa dumneavoastră de e-mail.
- **Scanează fişierele 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.

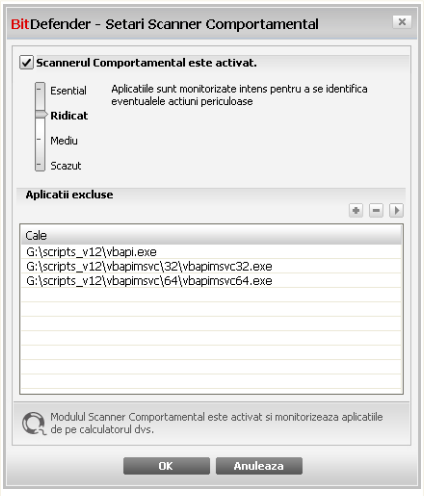


Alertă motor de scanare comportamental

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.

Notă
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

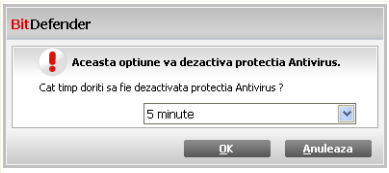
Puteți configura motorul comportamental de scanare să nu verifice anumite aplicații. Pentru a activa această protecție selectați căsuța corespunzătoare opțiunii **Activează controlul aplicațiilor**.

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.

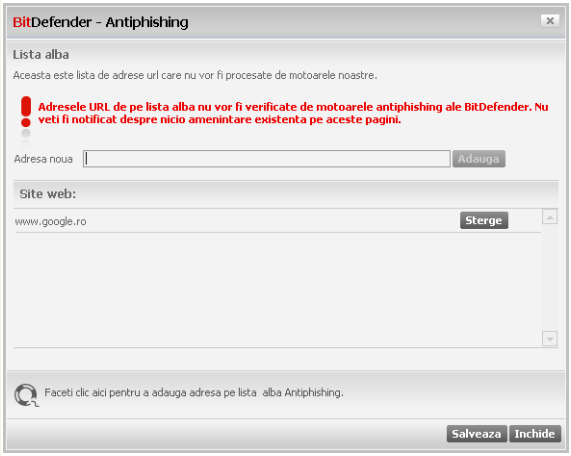
15.1.5. Configurarea protecției antiphishing

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.

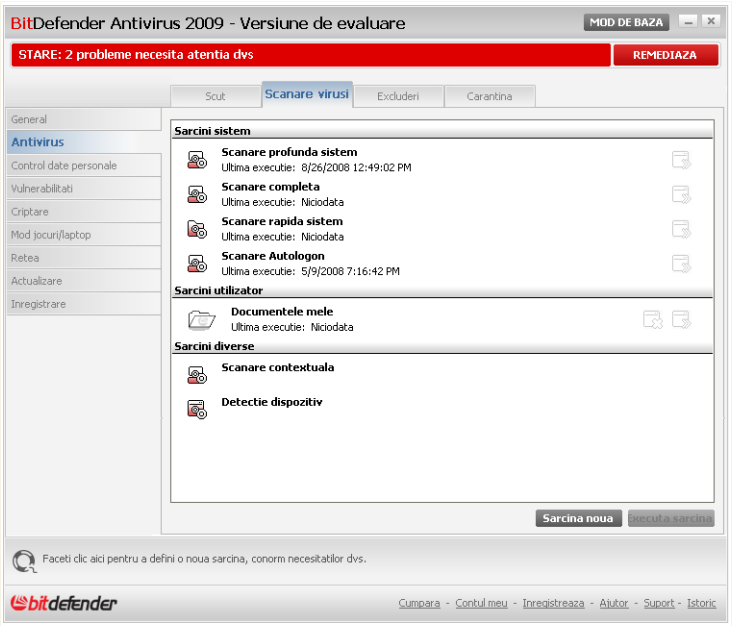
Faceți clic pe **Închide** pentru a salva modificările şi închide fereastra.

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. 116).

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 rulaţi aceste sarcini cu prioritate scăzută sau, şi mai bine, atunci când nu utilizaţi calculatorul.

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

  O sarcină denumită `Documentele mele` este furnizată. Utilizaţi această sarcină pentru a scana directoare importante ale utilizatorului curent: `My Documents`, `Desktop` şi `StartUp`. Astfel, veţi asigura siguranţa documentelor dumneavoastră, un spaţiu de lucru sigur şi rularea la pornirea sistemului a unor aplicaţii necompromise.
- **Sarcini diverse** - conţine 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. Puteţi doar să modificaţi setările acestora şi să examinaţi 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. Faceţi clic pe acest buton pentru a deschide fereastra de **Proprietăţi** la tabul Planificare, unde puteţi vedea şi modifica programul de rulare a sarcinii.
- **Şterge** - şterge sarcina selectată.

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

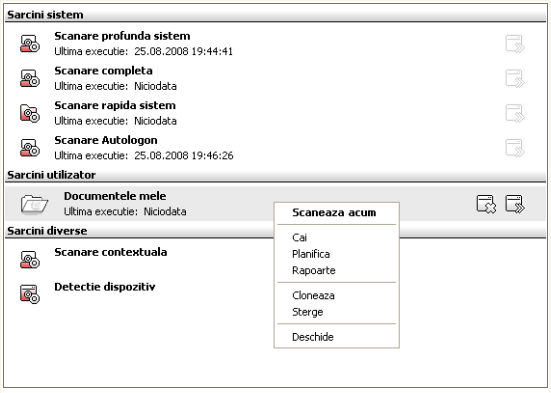
- **Scanare** - execută sarcina selectată, pornind o scanare imediată.

În partea stângă a fiecărei sarcini, puteţi vedea butonul **Proprietăţi** care vă permite să configuraţi sarcina şi să vedeţi 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.

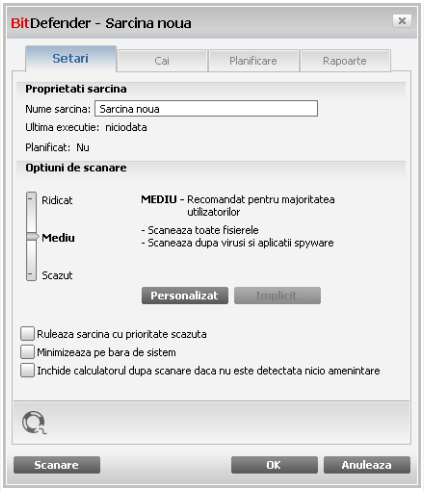
15.2.4. Configurarea sarcinilor de scanare

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. 135).

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:

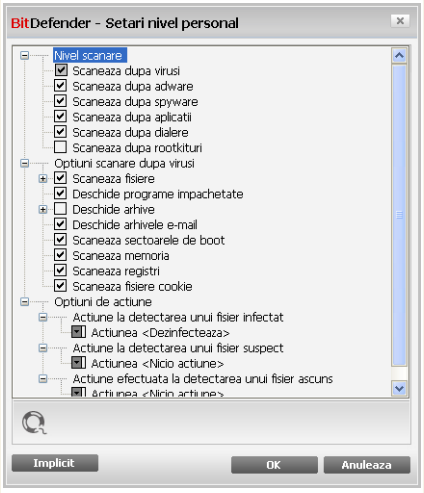
- **Rulează sarcina cu prioritate scăzută.** Reduce prioritatea procesului de scanare. Veţi permite altor programe să ruleze cu o viteză superioară, dar timpul necesar pentru finalizarea scanării va creşte.
- **Minimizează fereastra de scanare la bara de scanare.** Minimizează fereastra de scanare bara 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:

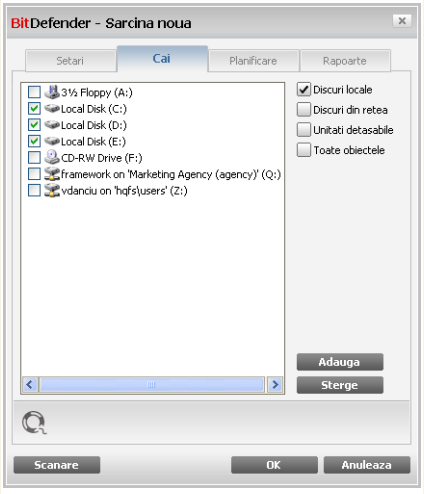
Acțiune	Descriere
Înregistrează ca nefiind scanate	Doar ține evidența fişierelor protejate prin parolă în raportul de scanare. După finalizarea scanării, puteți deschide raportul de scanare pentru a vedea informații despre aceste fişiere.
Cere parola	Atunci când este detectat un fişier protejat prin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

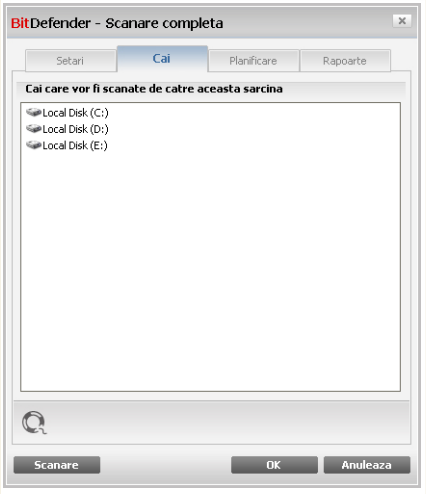
Notă
Dacă doriți să vă scanați tot sistemul, selectați opțiunea **Toate obiectele**.

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

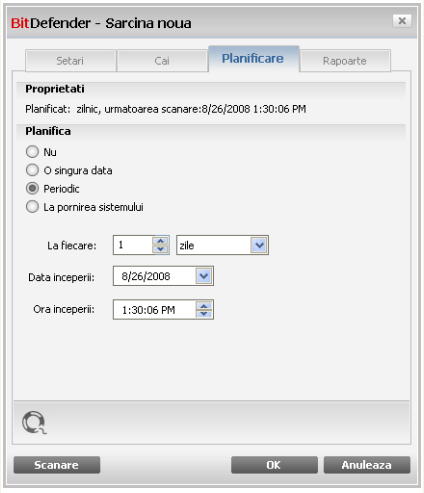
Sarcinile **Scanare completă sistem** şi **Scanare profundă sistem** scanează toate partițiile locale, în timp ce sarcina **Scanare rapidă sistem** scanează doar directoarele `Windows` şi `Program Files`.

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.

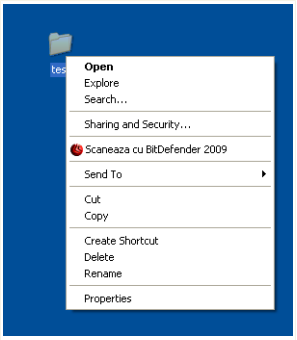
Pentru a rula o sarcină de scanare, utilizați una dintre următoarele metode:

- 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. 131).

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

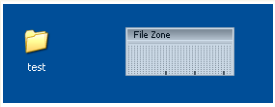
Faceți clic-dreapta pe fişierul sau directorul care doriți să fie scanat şi selectați opțiunea **BitDefender Antivirus 2009**.

Va apărea programul asistent de scanare şi scanarea va fi inițiată. Pentru mai multe informații, consultați "*Programul asistent de scanare*" (p. 131).

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 fişierul

Lăsați fişierul

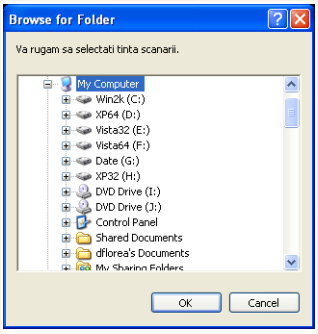
Va apărea programul asistent de scanare şi scanarea va fi inițiată. Pentru mai multe informații, consultați "*Programul asistent de scanare*" (p. 131).

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**.

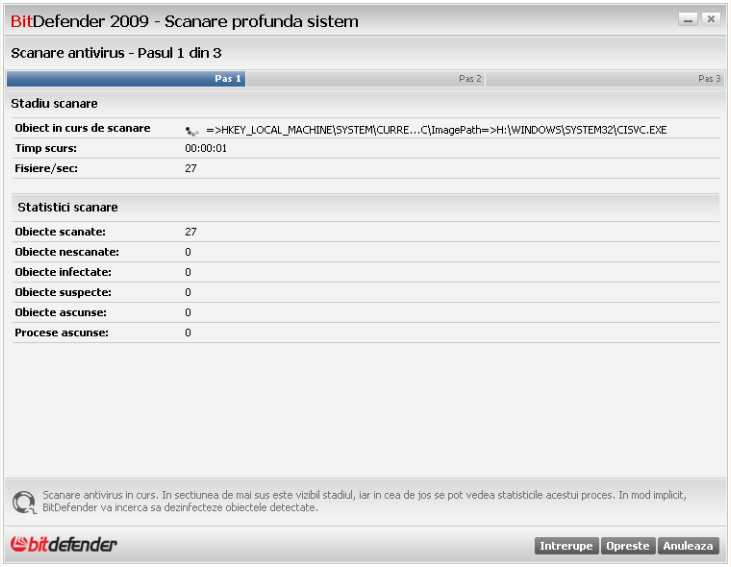
Va apărea programul asistent de scanare şi scanarea va fi inițiată. Pentru mai multe informații, consultați "*Programul asistent de scanare*" (p. 131).

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.

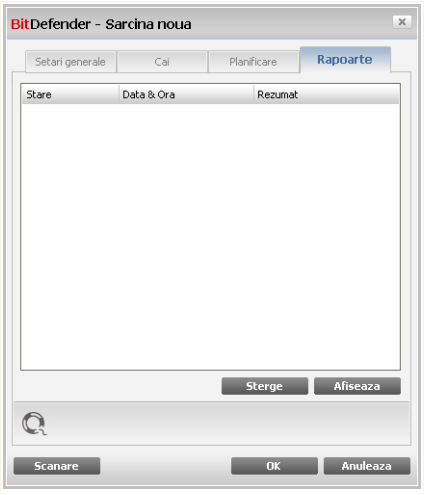
BitDefender a detectat fişiere suspecte

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:

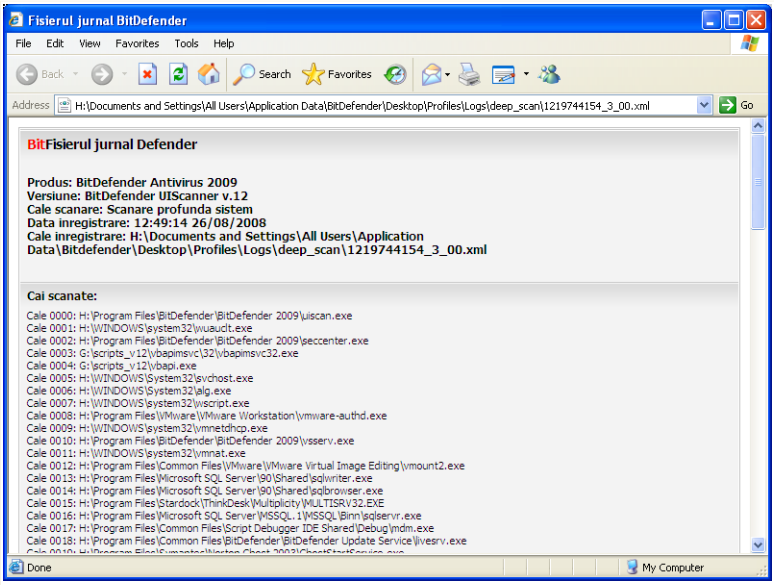
- **Şterge** - şterge fişierul de raport selectat.
- **Afişează** - deschide fişierul de raport selectat. Raportul de scanare va fi deschis în browserul dumneavoastră implicit.

Notă
De asemenea, pentru a deschide sau şterge un fişier de raport, faceţi clic-dreapta pe fişier şi selectaţi opţiunea corespunzătoare din meniu.

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

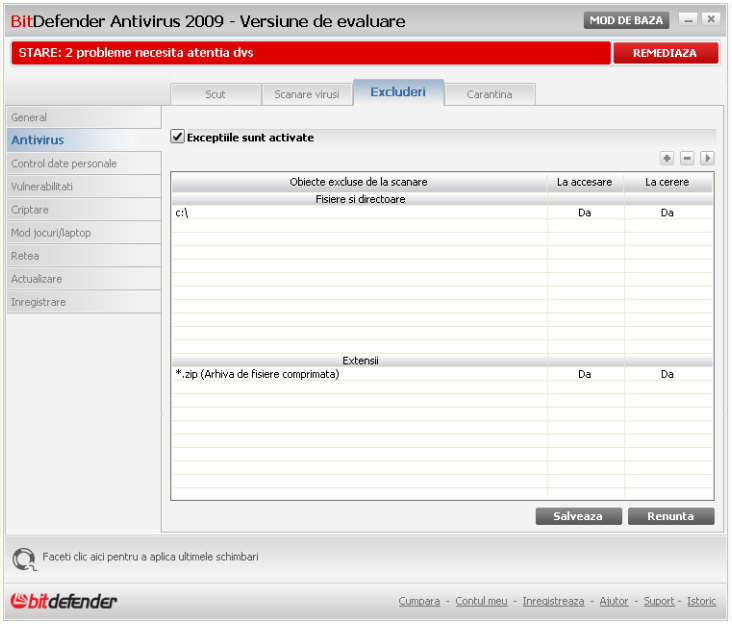
BitDefender permite excluderea obiectelor atât de la scanarea la acces, cât şi de la scanarea la cerere. Această caracteristică este menită să reducă timpul de scanare şi să evite orice fel de interferență cu munca dumneavostră.

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.

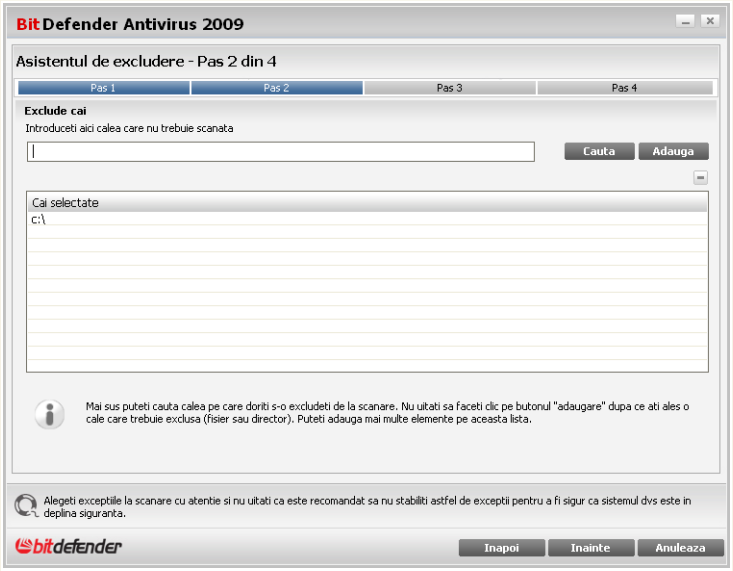
Pasul 1/4 - Selectați tipul obiectului

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**.

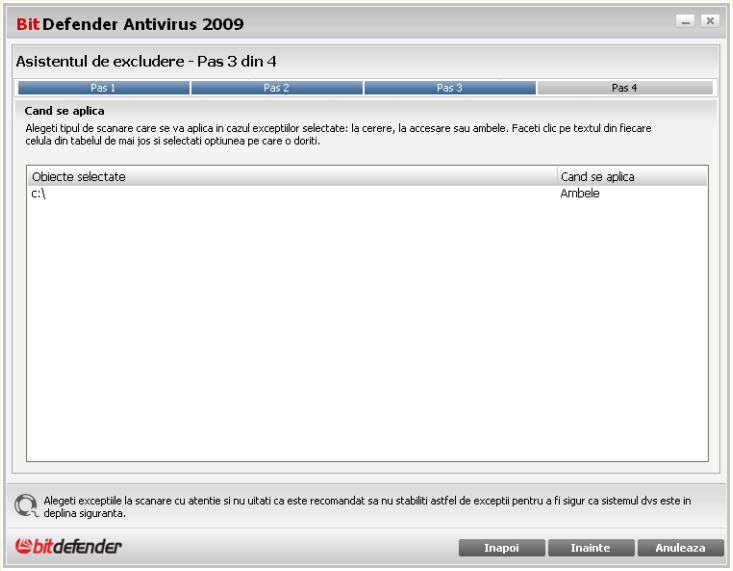
Notă
Un mesaj de eroare va apărea dacă nu există calea furnizată. Faceți clic pe **OK** şi verificați validitatea căii.

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.

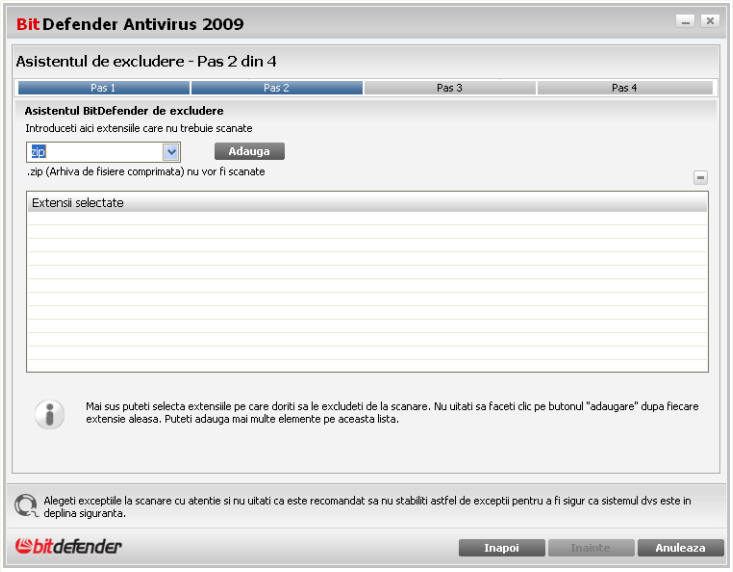
Pasul 1/4 - Selectați tipul obiectului

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.

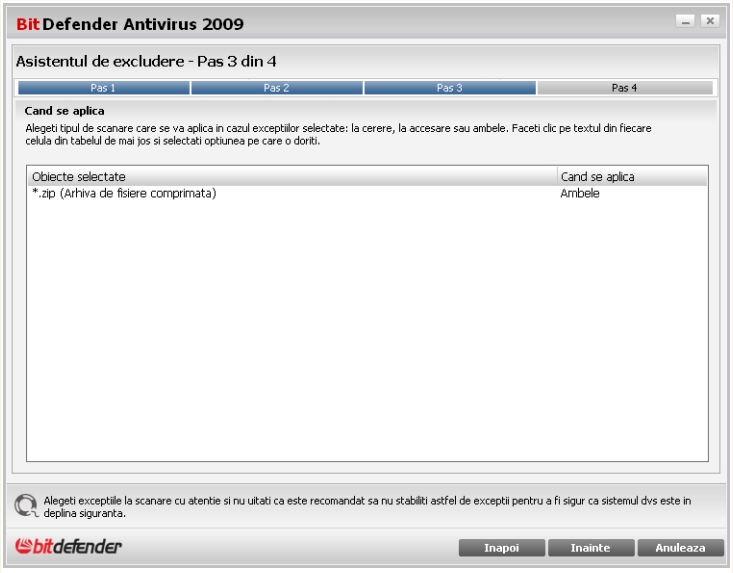
- Introduceți extensia care doriți să fie exclusă de la scanare şi faceți clic pe **Adaugă**.

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.

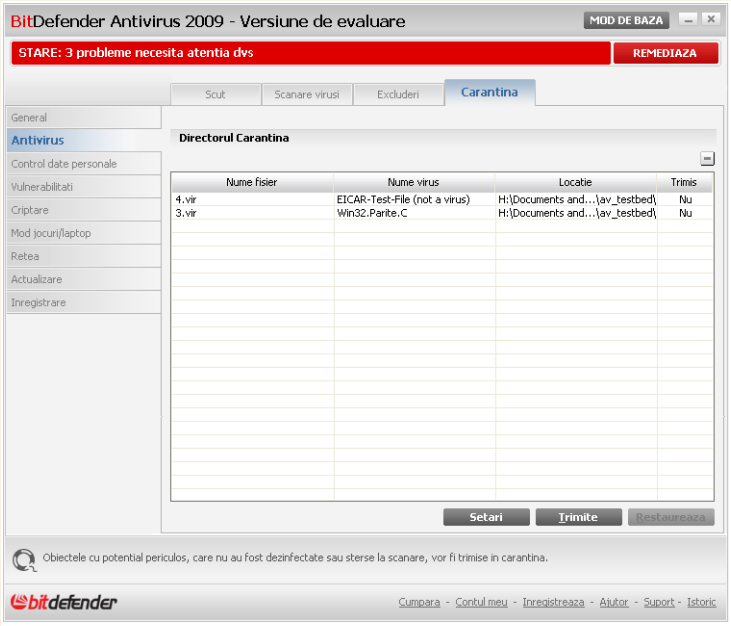
Faceți clic pe **Finalizare**.

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

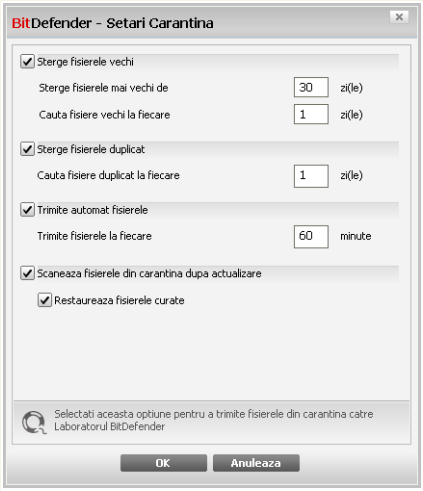
Pentru a şterge un fişier selectat din carantină faceți clic pe butonul **Şterge**. Dacă doriți să mutați fişierul selectat la locația originală faceți clic pe **Restaurează**.

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

Meniul contextual. Un meniu contextual este disponibil, permițând gestionarea rapidă a fişierelor 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**.

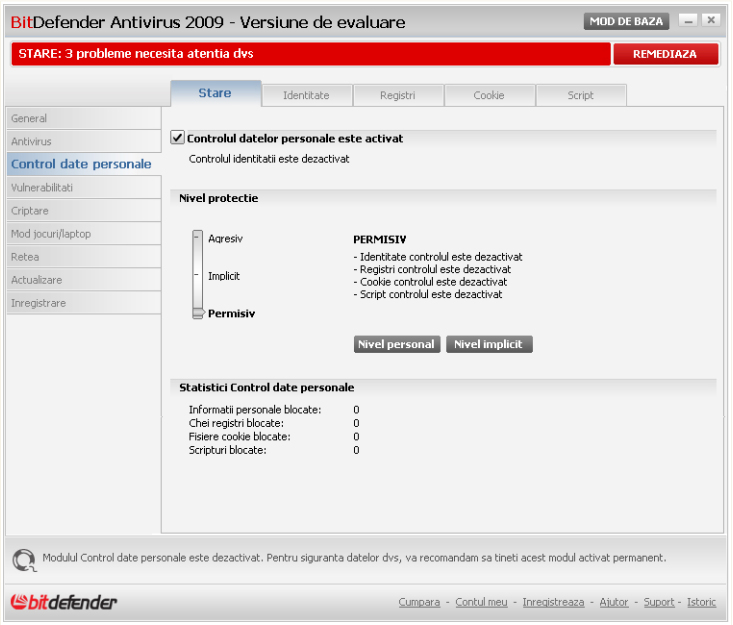
Faceți clic pe **OK** pentru a salva modificările şi închide fereastra.

16. 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.

16.1. 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**.

16.1.1. 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.

16.2. 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.

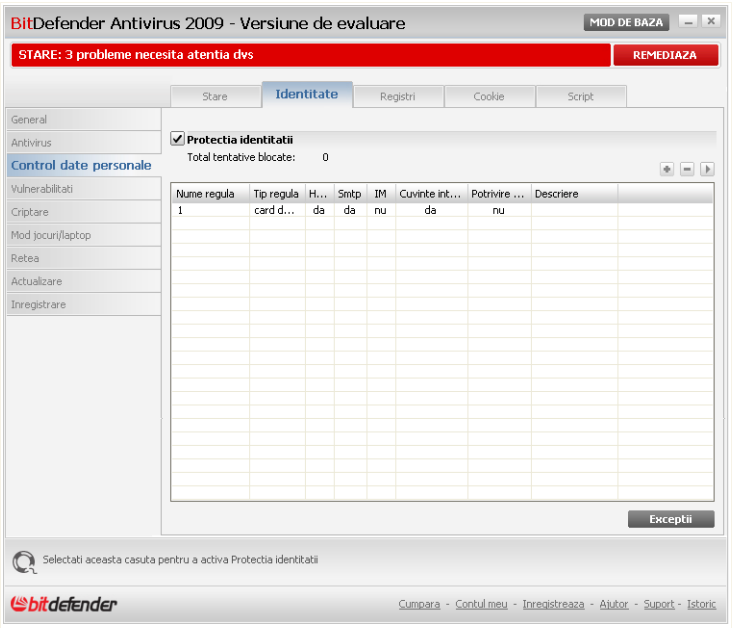
  În eventualitatea în care o astfel de aplicație reuşeşte să evite detecția antivirus, aceasta nu va putea trimite datele furate prin e-mail, web sau mesaje instant, dacă ați creat reguli adecvate de protecție a identității.

- 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

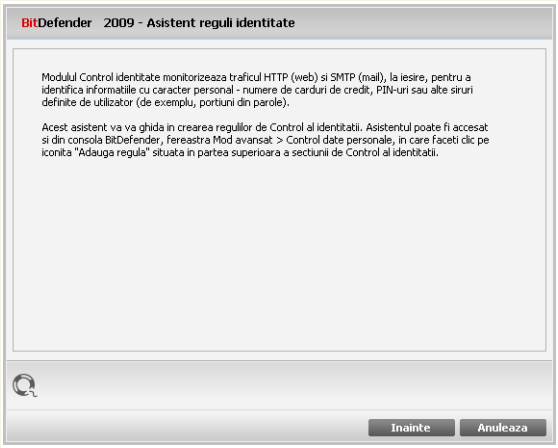
Dacă doriți să utilizați Controlul identității, urmați aceşti paşi:

1. Selectați căsuța **Control identitate**.
2. Creați reguli pentru a vă proteja datele confidențiale. Pentru mai multe informații, consultați "*Crearea regulilor de identitate*" (p. 154).
3. Daca este nevoie, definiți excepții specifice de la regulile pe care le-ați creat. Pentru mai multe informații, consultați "*Specificarea excepțiilor*" (p. 157).

16.2.1. 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:

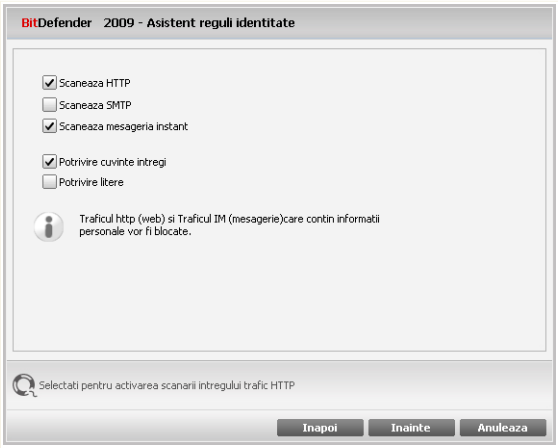
- **Nume regulă** - introduceți numele regulii în acest câmp editabil.
- **Tip regulă** - alegeți tipul regulei (adresă, nume, card de credit, PIN, etc.).
- **Date regulă** - introduceți datele pe care doriți să le protejați în acest câmp editabil. De exemplu, pentru a vă proteja numărul cardului dumneavoastră 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

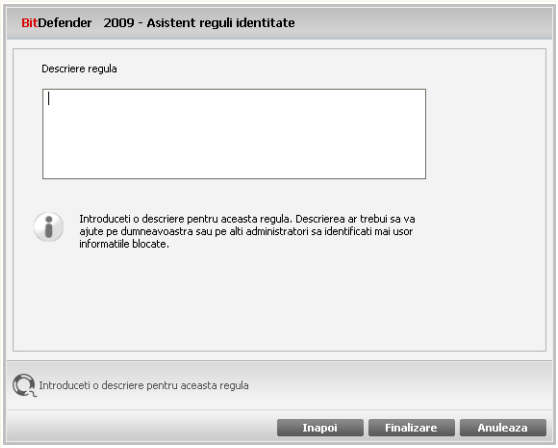
Selectați tipul de trafic care doriți să fie scanat de BitDefender. Următoarele opțiuni sunt disponibile:

- **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

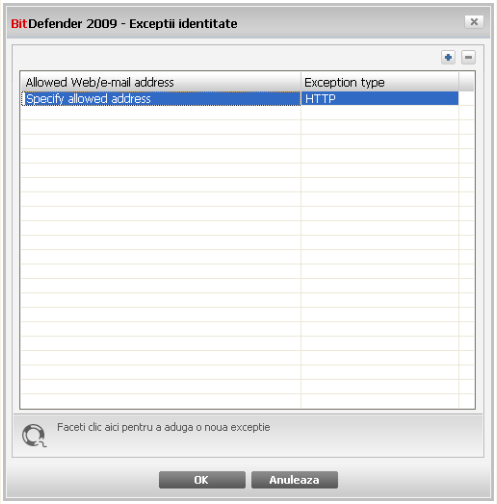
Introduceți o scurtă descriere a regulei în câmpul editabil. Deoarece informația blocată (şirul respectiv de caractere) nu este afişată atunci când este accesată regula, descrierea trebuie să ajute la identificarea acesteia.

Faceți clic pe **Finalizare**. Regula va apărea în tabel.

16.2.2. 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**.

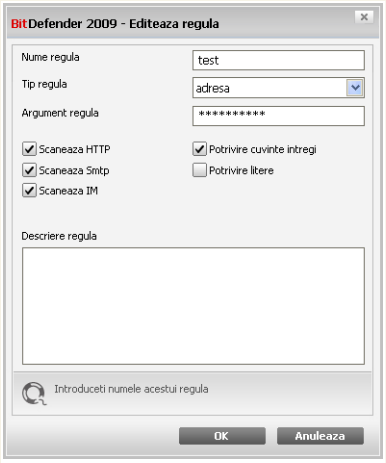
Faceți clic pe **OK** pentru a salva modificările.

16.2.3. 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

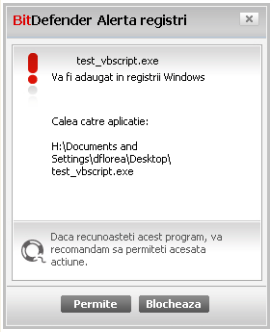
Aici puteți modifica numele, descrierea şi parametrii regulei (tip, argument şi trafic). Faceți clic pe **OK** pentru a salva modificările.

16.3. 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.

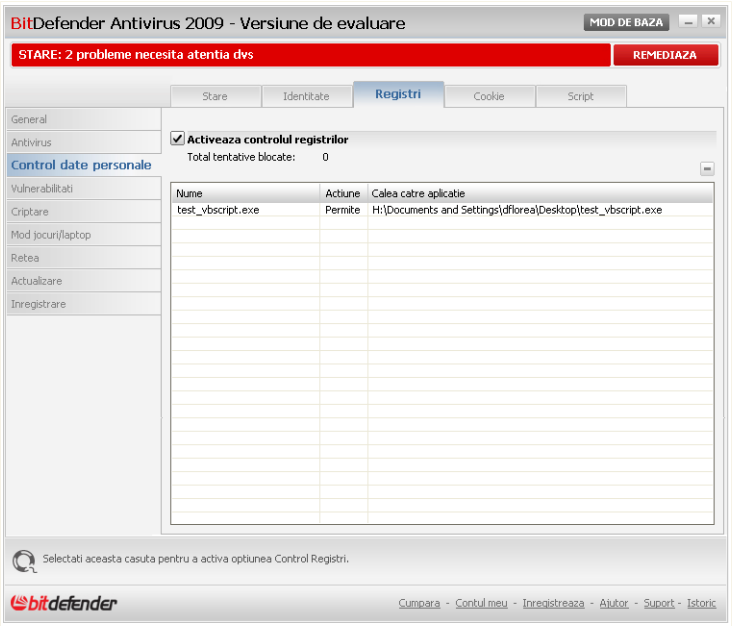
Dacă nu recunoaşteți programul şi acesta pare suspect, faceți clic pe **Blochează** pentru a-l împiedica să modifice regiştrii Windows. Altfel, faceți clic pe **Permite** pentru a permite modificarea.

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**.

16.4. 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.

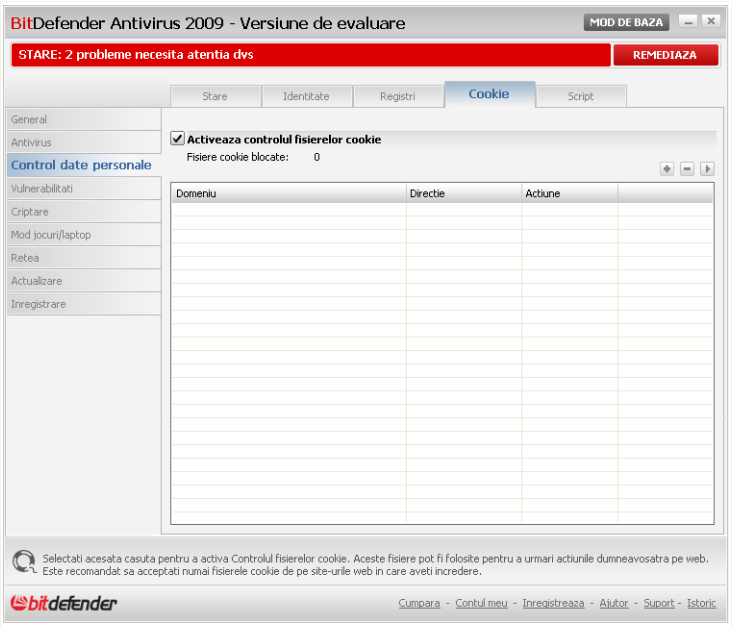
Selectați opțiunea **Reține acest răspuns** şi faceți clic pe **Da** sau **Nu** şi o regulă va fi creată, aplicată şi afişată în lista de reguli. Data viitoare când vă veți conecta la acelaşi site nu veți mai fi notificat.

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.

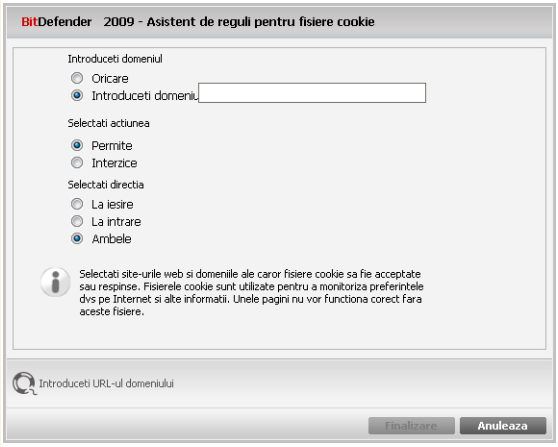
Important
Regulile sunt listate în ordinea priorității începând de sus, adică prima regulă are cea mai mare prioritate. Mutați regulile în sus sau în jos pentru a le schimba prioritatea.

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.

16.4.1. 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**.

16.5. 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.

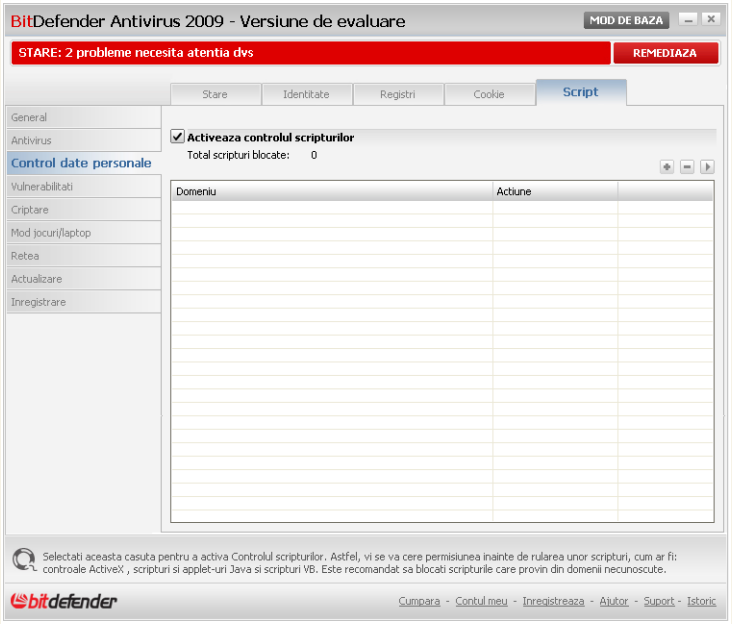
Având **Controlul scripturilor** activat, veți monitoriza adresele web în care aveți încredere şi pe cele în care nu aveți. BitDefender vă va cere permisiunea de fiecare dată când un domeniu încearcă să ruleze un script sau alt conținut activ:

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.

16.5.1. 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**.

17. 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.

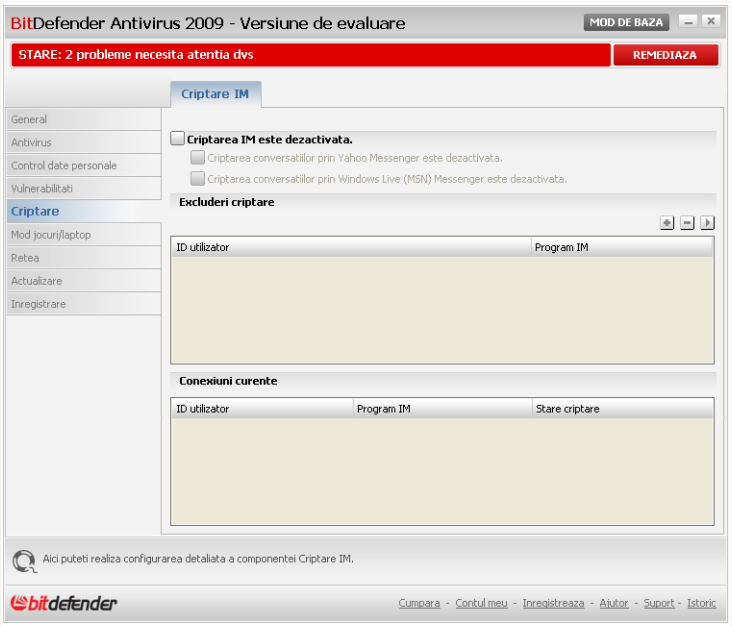
Important

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. 35).



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.

17.1. 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**.

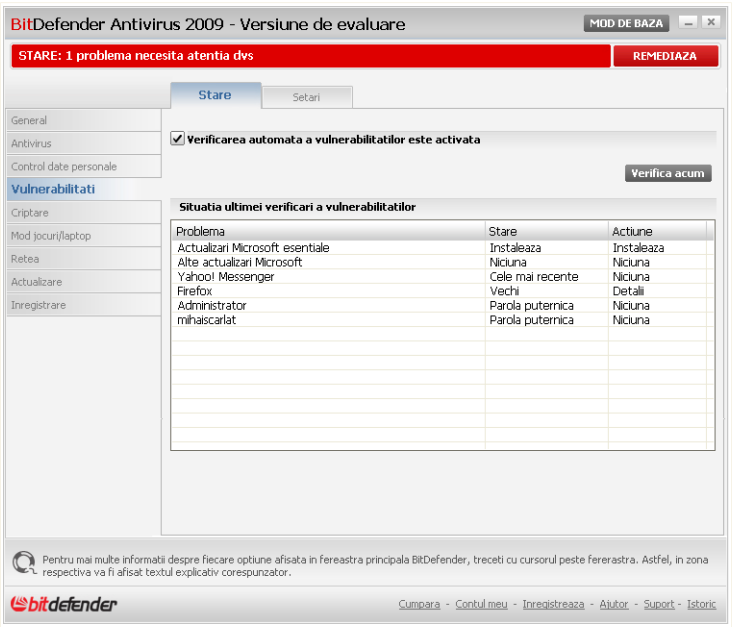
18. Vulnerabilitate

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.

18.1. 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.

18.1.1. Căutare după vulnerabilități

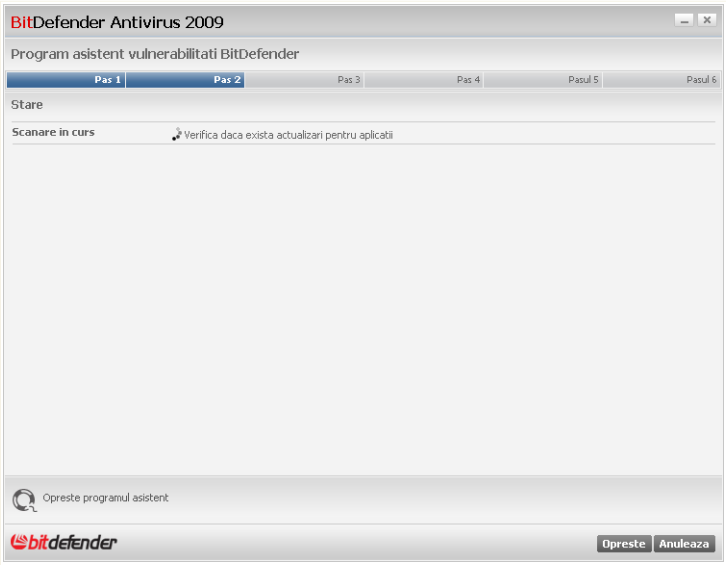
Pentru a verifica dacă sistemul dumneavoastră este vulnerabil, faceți clic pe **Verifică acum** şi urmați paşii programului asistent.

Pasul 1/6 - Selectați vulnerabilitățile de verificat

Vulnerabilități

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

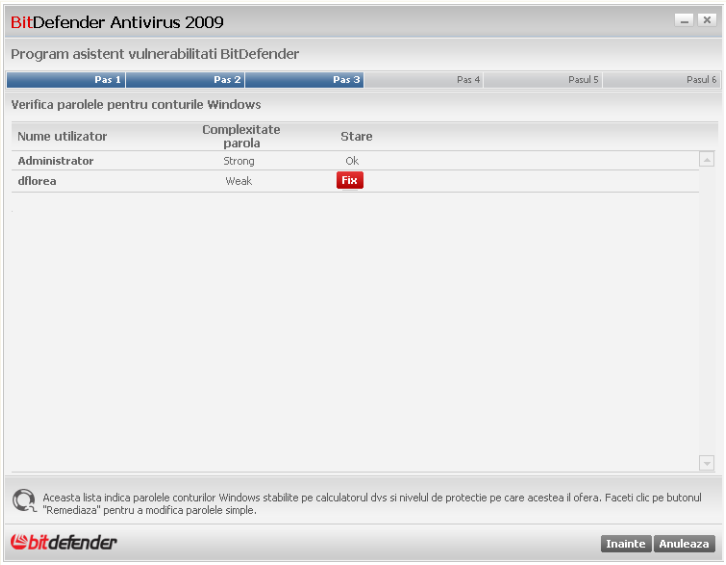
Pasul 2/6 - Căutare vulnerabilități



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:

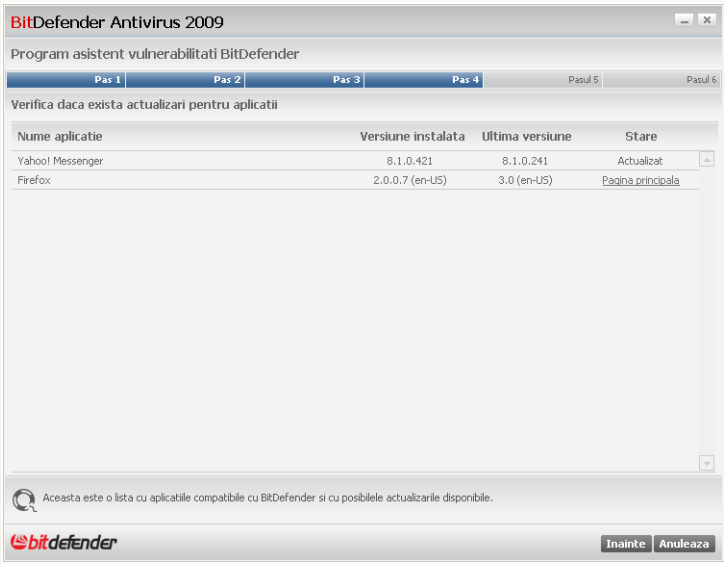
- **Forțează utilizatorul să schimbe parola la următoarea conectare.** BitDefender va cere utilizatorului să schimbe parola data viitoare când acesta se conectează la contul său Windows.
- **Schimbă parola utilizatorului.** Trebuie să introduceți noua parolă în câmpurile editabile.

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

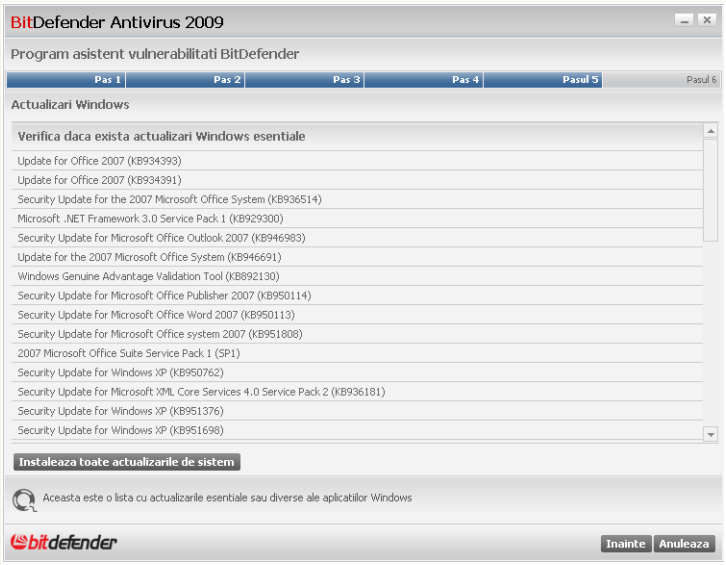


Aplicații

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**.

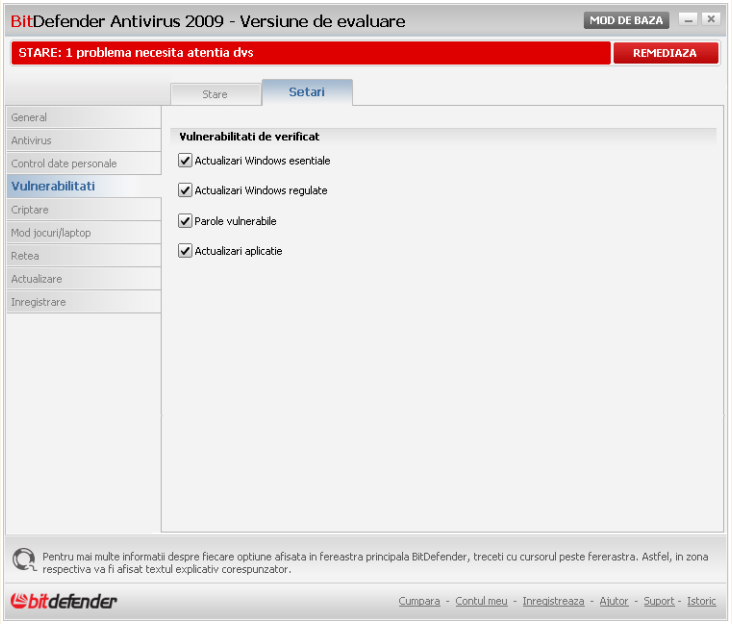
Pasul 6/6 - Examinați rezultatele

Rezultate

Faceți clic pe **Închide**.

18.2. 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.

19. 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.

19.1. 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**.
- Actualizările nu sunt efectuate în mod implicit.

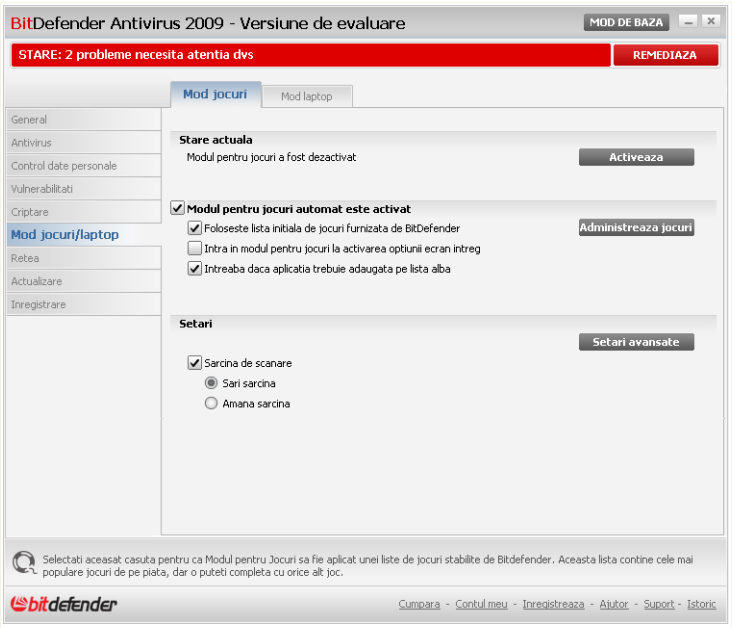
Notă
Pentru a modifica această setare, mergeți la Actualizare>Setări şi debifați căsuța **Nu actualiza dacă este activat modul pentru jocuri**.

- Sarcinile de scanare programate sunt dezactivate în mod implicit.

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`).

Notă
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.

19.1.1. 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:

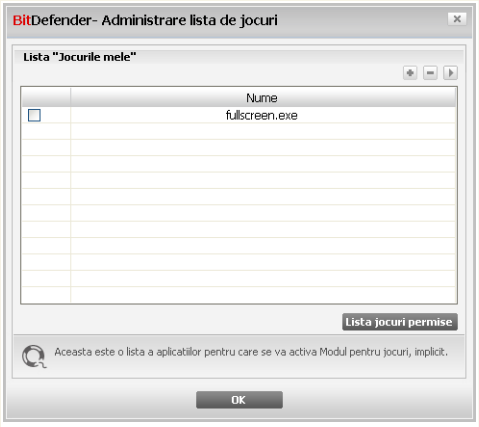
- **Utilizează lista de jocuri furnizată de BitDefender** - pentru a intra automat în modul pentru jocuri când porniți un joc din lista de jocuri cunoscute a BitDefender. Pentru a vedea această listă, faceți clic pe **Administrare jocuri** şi apoi pe **Afişează jocuri permise**.

- **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**.

19.1.2. 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, adăugaţi aplicaţia în lista de jocuri prin intermediul ferestrei de alertă.

Dacă doriţi să dezactivaţi modul automat pentru jocuri pentru o anumită aplicaţie din listă, debifaţi căsuţa corespunzătoare acesteia. Puteţi dezactiva modul automat pentru jocuri pentru aplicaţii normale care intră în full screen, cum ar fi browserele web şi programele de vizionat filme.

Pentru a administra lista de jocuri, puteţi 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 adăugaţi sau editaţi o înregistrare din lista de jocuri, va apărea următoarea fereastră:

Adaugă joc

Faceţi clic pe **Caută** pentru a selecta aplicaţia sau introduceţi calea completă către aplicaţie în câmpul editabil.

Dacă nu doriţi ca BitDefender să intre automat în modul pentru jocuri atunci când aplicaţia selectată este pornită, selectaţi **Dezactivează**.

Faceţi clic pe **OK** pentru a adăuga înregistrarea în lista de jocuri.

19.1.3. 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.

19.1.4. 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.

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

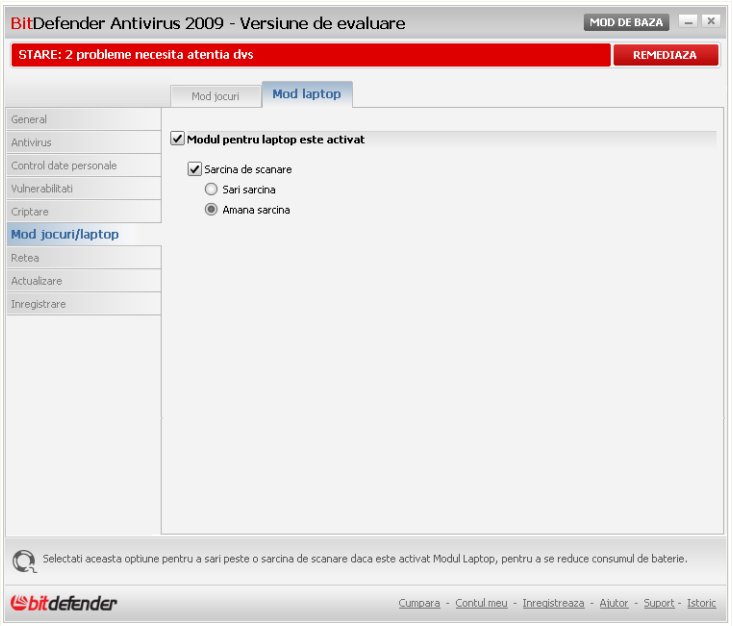
19.2. Modul pentru laptop

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.

19.2.1. Configurarea setărilor modului pentru laptop

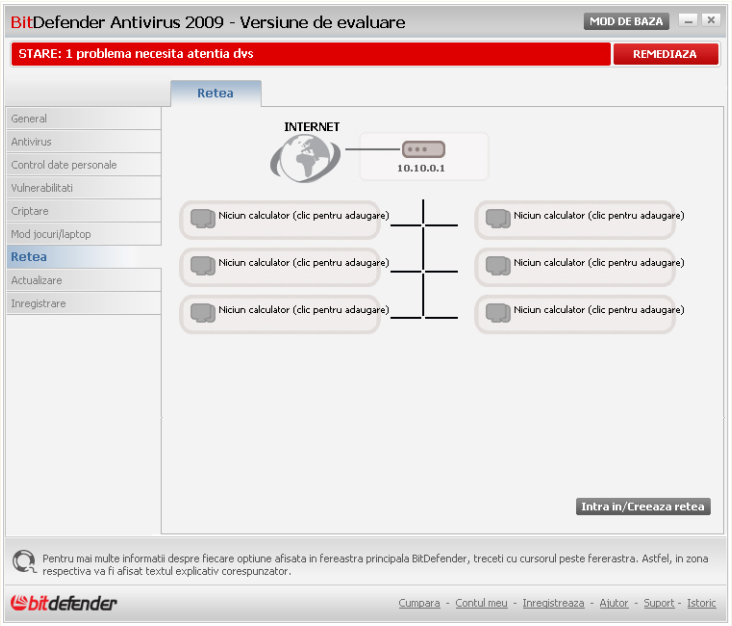
Pentru a configura executarea sarcinilor programate, utilizați aceste opțiuni:

- **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.

20. Rețea

Modulul Rețea vă permite să administrați produsele BitDefender instalate pe calculatoarele personale de pe un singur calculator.



Hartă rețea

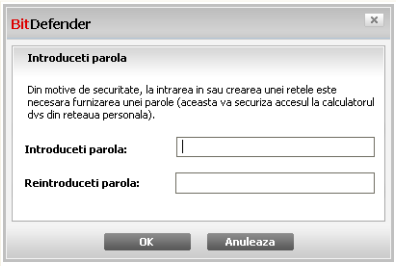
Pentru a putea administra produsele BitDefender instalate pe calculatoarele personale, trebuie să urmați aceşti paşi:

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.

20.1. 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**.

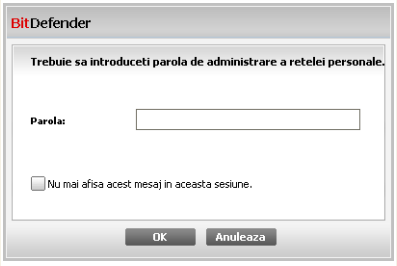
Puteți vedea numele calculatorului apărând pe harta rețelei.

20.2. 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.

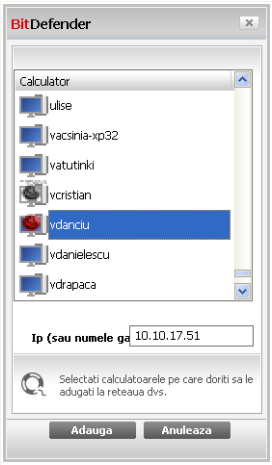
Pentru a adăuga un calculator la rețeaua BitDefender personală, urmați aceşti paşi:

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.



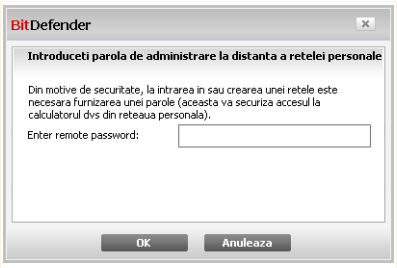
Adaugare calculator

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.



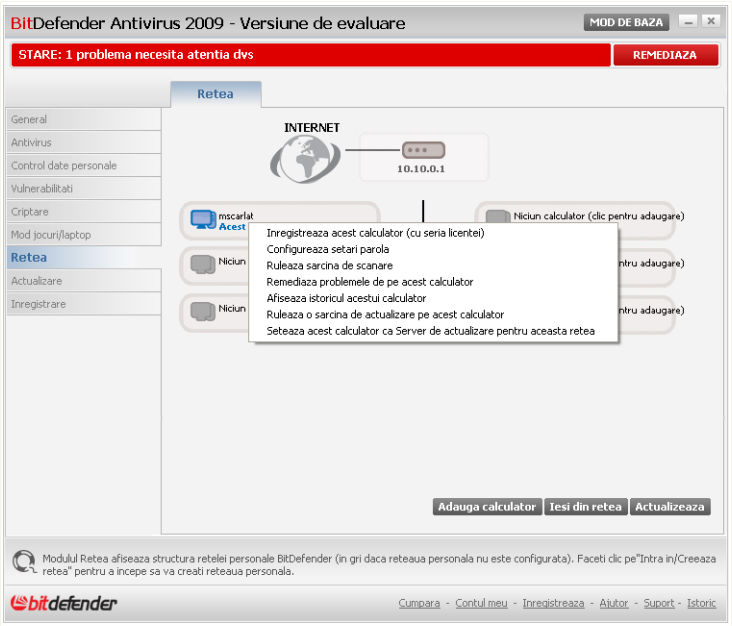
Autentificare

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.

20.3. Administrarea rețelei BitDefender

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



Hartă rețea

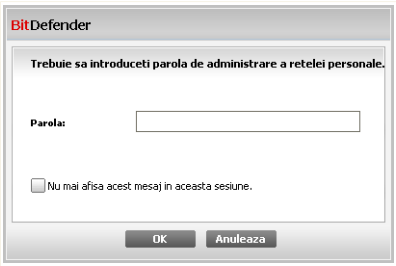
Dacă plasați cursorul mouse-ului deasupra unui calculator de pe harta rețelei, puteți vedea informații sumare despre acesta (nume, adresă IP, numărul de probleme care afectează securitatea sistemului, starea înregistrării).

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.

21. 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.

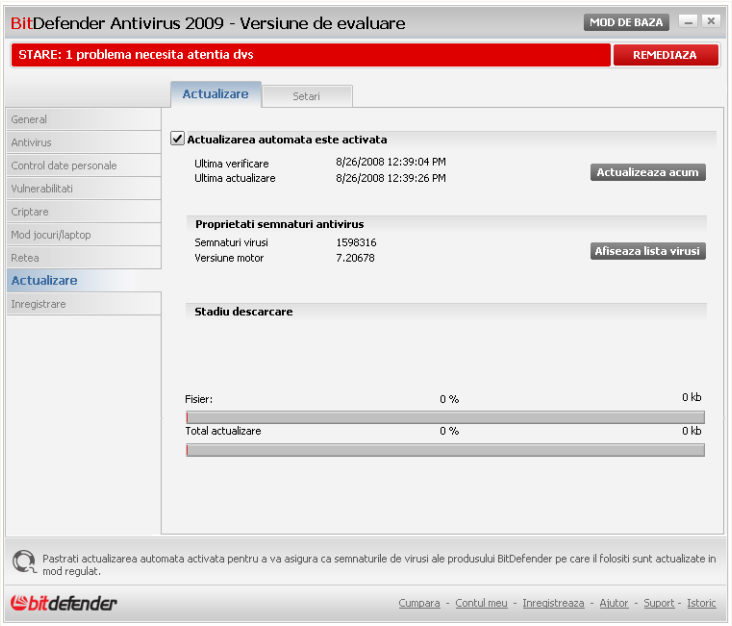
Procesul de actualizare este realizat progresiv, ceea ce inseamna ca fisierele care trebuie actualizate sunt inlocuite unul cate unul. Astfel, procesul de actualizare nu va afecta funcţionarea produsului şi, în acelaşi timp, orice vulnerabilitate va fi exclusă.

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 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**.

21.1. 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.

21.1.1. 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**.

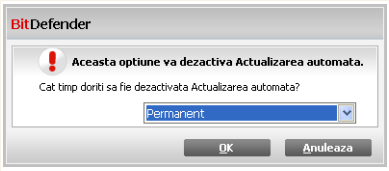
Modulul **Actualizare** se va conecta la serverul de actualizare BitDefender şi va verifica dacă sunt disponibile noi semnături. Dacă sunt detectate noi semnături, în funcție de opțiunile setate în secțiunea Setări actualizare la cerere, vi se va cere să confirmați actualizarea sau aceasta va fi realizată 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.

21.1.2. Dezactivarea actualizării automate

Dacă doriți să dezactivați actualizarea automată, va apărea o fereastră de avertizare.



Dezactivează actualizarea automată

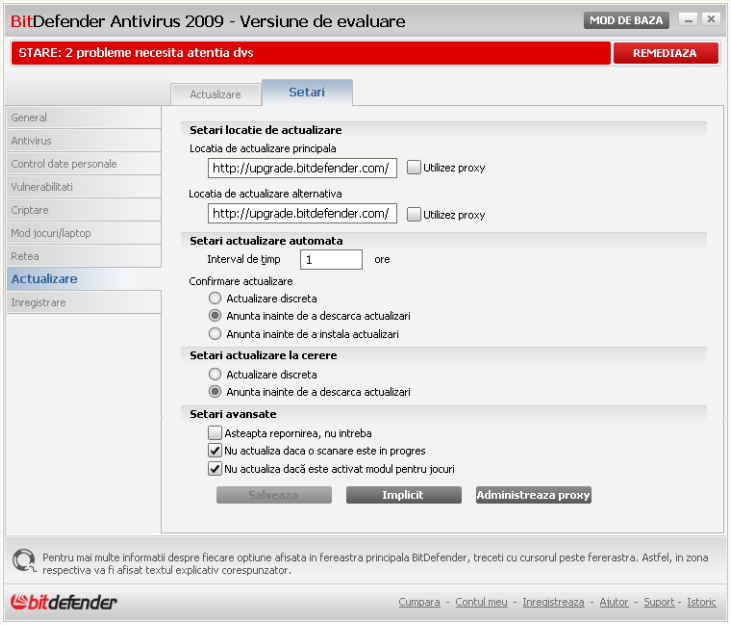
Va trebui să confirmați acțiunea selectând din meniu intervalul de timp pentru care să fie dezactivată actualizarea automată. Puteți dezactiva actualizarea automată pentru 5, 15 sau 30 minute, pentru o oră, permanent sau doar până la repornirea sistemului.

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.

21.2. 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.

21.2.1. 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. 198).

21.2.2. 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.

21.2.3. 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.

21.2.4. 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.

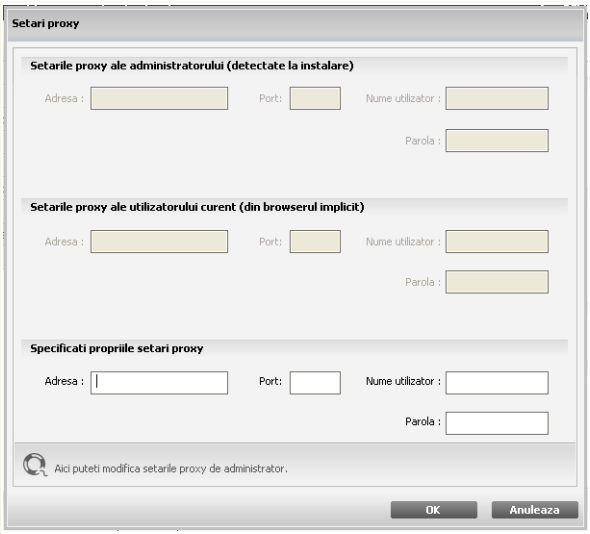
- **Nu actualiza dacă este activat modul pentru jocuri** - BitDefender nu se va actualiza dacă funcționează în modul pentru jocuri. Astfel, puteți minimiza influența produsului asupra performanțelor sistemului în timpul jocului.

21.2.5. Administrarea proxy-urilor

În cazul în care compania utilizează un server proxy pentru conectarea la Internet, trebuie să specificați setările proxy pentru ca BitDefender să se poată actualiza. Altfel, BitDefender va utiliza setările proxy ale administratorului care a instalat produsul sau ale browserului implicit al utilizatorului curent, dacă acestea există.

Notă
Setările proxy pot fi configurate doar de utilizatori cu drepturi administrative pe calculator sau de către utilizatori care cunosc parola produsului.

Pentru a 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.

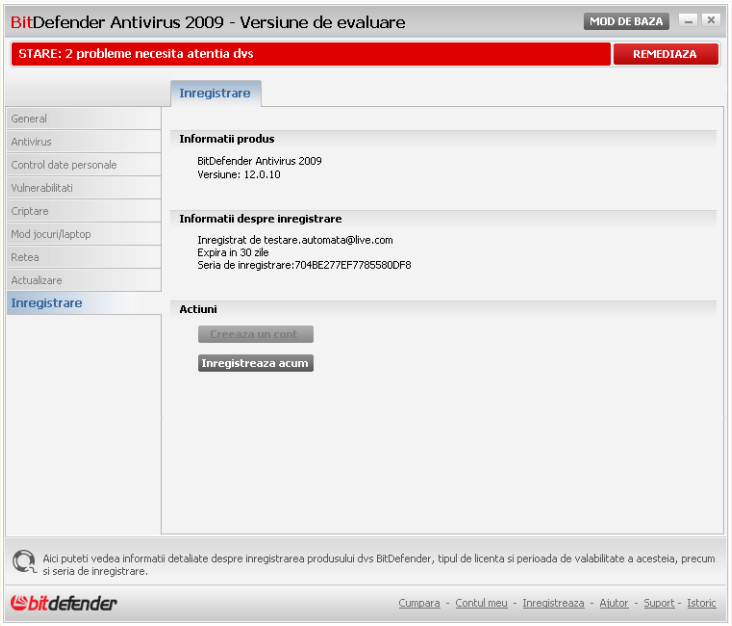
Mai întâi, va fi utilizat setul conţinând propriile dumneavoastre setări proxy pentru conectarea la Internet. Dacă acesta nu merge, vor fi încercate în continuare setările proxy detectate la instalare. În sfârşit, dacă nici acestea nu sunt bune, vor fi extrase setările proxy ale utilizatorului curent 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.

22. Înregistrare

Pentru a afla informații complete despre produsul dumneavoastră BitDefender şi despre starea înregistrării, mergeți la **Înregistrare** în modul avansat.



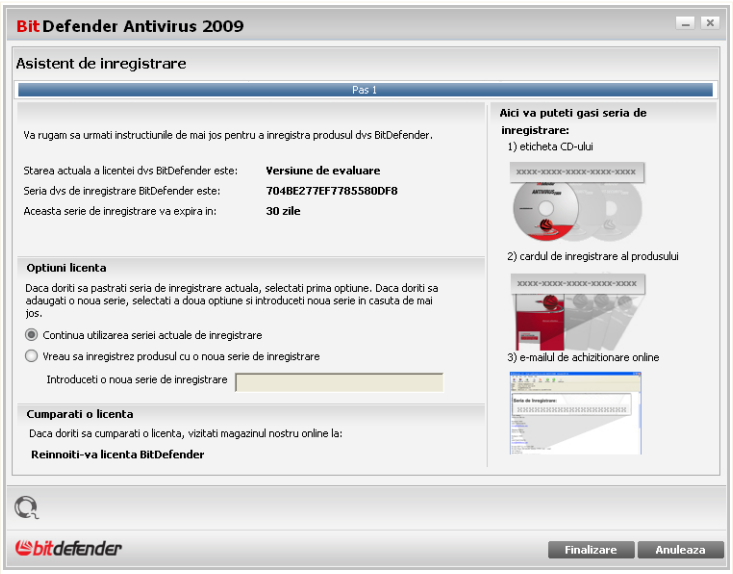
Înregistrare

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.

22.1. Înregistrarea BitDefender Antivirus 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 Antivirus 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**.

22.2. 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. 204)
- “Deja am un cont BitDefender” (p. 205)

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

23. 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.

23.1. 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.

23.2. Solicitarea ajutorului

23.2.1. 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/

23.2.2. 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/

23.3. 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.

23.3.1. 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

23.3.2. 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

24. Descriere generală

BitDefender Antivirus 2009 este furnizat cu un CD de boot (BitDefender Rescue CD) capabil a scana şi dezinfecta tot calculatorul fără a 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/

24.1. 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.

24.2. 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.

25. 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.

25.1. 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

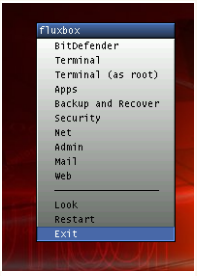
La pornirea sistemului, se face automat actualizarea semnăturilor de viruşi. Procesul poate lua ceva timp.

La finalizarea procesului de pornire veți vedea următorul desktop. Acum puteți începe să utilizați BitDefender Rescue CD.

Desktopul

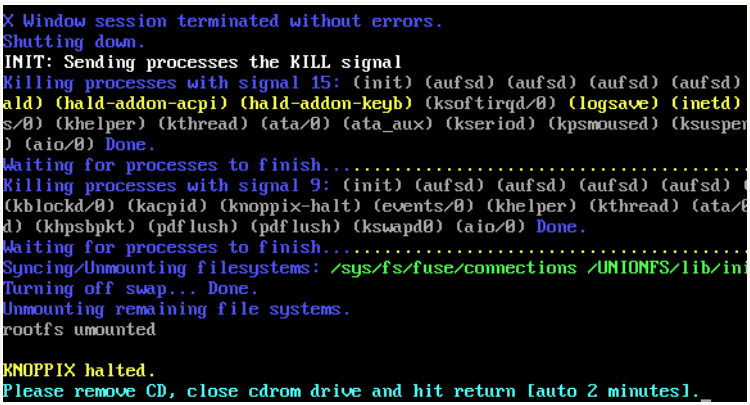
25.2. Oprirea BitDefender Rescue CD

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

25.3. 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**.

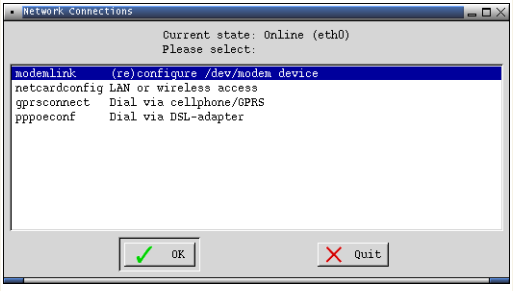
Sau puteţi iniţializa următoarea comandă de la un terminal. **BitDefender Antivirus Scanner** va începe cu fişierul sau directorul selectat ca locaţie implicită de scanare.

```
# bdscan /path/to/scan/
```

25.4. 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:

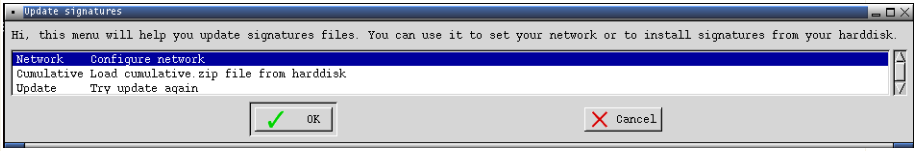
```
# pppconfig
```

4. Urmați instrucțiunile de pe ecran. Dacă nu ştiți ce să scrieți, contactați administratorul sistemului sau rețelei dumneavoastră pentru detalii.

25.5. 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**.

25.5.1. 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**.

25.6. 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

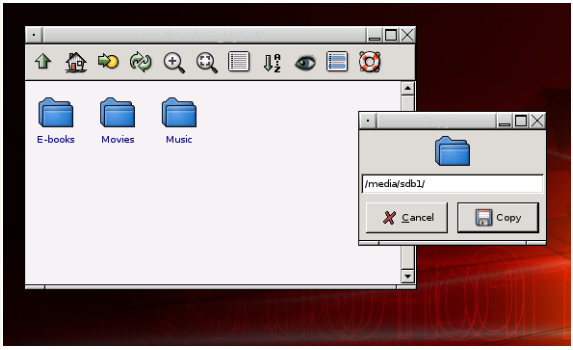
3. Faceți dublu-clic pe partiția unde se află datele pe care vreți să le salvați (de exemplu, `[sda3]`).

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.