



bitdefender
antivirus **2010**

Manual de utilizare

BitDefender Antivirus 2010 *Manual de utilizare*

Publicat 2010.04.20

Copyright© 2010 BitDefender

Termeni legali

Toate drepturile rezervate. Nicio parte a acestui document nu va putea fi reprodusă sau transmisă sub nicio formă și prin niciun mijloc, fie el electronic sau mecanic, inclusiv fotocopiere, înregistrare, sau orice sistem de stocare și recuperare de date, fără acordul scris al unui reprezentant autorizat al BitDefender. Este posibilă includerea unor scurte citate în recenzii, dar numai cu condiția menționării sursei citate. Conținutul documentului nu poate fi modificat în niciun fel.

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

Acest document conține linkuri către siteuri web aparținând unor terți, care nu se află sub controlul BitDefender; prin urmare, BitDefender nu este responsabilă pentru conținutul respectivelor siteuri. Responsabilitatea accesării oricăruia dintre siteurile terților al căror link este furnizat în acest document vă aparține în totalitate. Aceste linkuri sunt furnizate exclusiv pentru ușurarea consultării documentului și prezența lor nu presupune faptul că BitDefender susține sau își asumă responsabilitatea pentru conținutul siteurilor către care duc acestea.

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



Cuprins

Contract de licență pentru utilizatorul final	ix
Prefață	xv
1. Convenții utilizate în manual	xv
1.1. Convenții tipografice	xv
1.2. Atenționări	xvi
2. Structura manualului	xvi
3. Comentarii	xvii
Instalare și dezinstalare	1
1. Cerințe de sistem	2
1.1. Cerințe de sistem minime	2
1.2. Cerințe de sistem recomandate	2
1.3. Aplicații în care se poate integra BitDefender	2
2. Pregătirea pentru instalare	4
3. Instalarea BitDefender	5
3.1. Asistentul de înregistrare	8
3.1.1. Pasul 1 - Înregistrați BitDefender Antivirus 2010	9
3.1.2. Pasul 2 - Creați un cont BitDefender	10
3.2. Asistentul de configurare	12
3.2.1. Pasul 1 - Selectați profilul de utilizator	13
3.2.2. Pasul 2 - Descrieți calculatorul	14
3.2.3. Pasul 3 - Selectați interfața	15
3.2.4. Pasul 4 - Configurați rețeaua BitDefender	16
3.2.5. Pasul 5 - Selectați sarcinile ce vor fi rulate	17
3.2.6. Pasul 6 - Finalizare	18
4. Actualizarea versiunii de produs	20
5. Repararea sau dezinstalarea BitDefender	21
Introducere	22
6. Descriere generală	23
6.1. Deschiderea BitDefender	23
6.2. Moduri de vizualizarea a interfeței cu utilizatorul	23
6.2.1. Modul Novice	24
6.2.2. Modul Intermediar	27
6.2.3. Modul Expert	28
6.3. Iconiță în bara de sistem	31
6.4. Bara de scanare	32
6.4.1. Scanare fișiere și directoare	32
6.4.2. Dezactivarea/Reactivarea barei de scanare	33
6.5. Scanare manuală BitDefender	33
6.6. Modul pentru jocuri și Modul pentru laptop	34
6.6.1. Modul pentru jocuri	35

6.6.2. Modul pentru laptop	36
6.7. Detecție automată unități	36
7. Remediere probleme	38
7.1. Asistent Remediere toate problemele	38
7.2. Configurarea monitorizării problemelor	40
8. Configurarea setărilor de bază	42
8.1. Setări interfață cu utilizatorul	43
8.2. Setări de securitate	44
8.3. Setări generale	45
9. Istoric și evenimente	47
10. Înregistrare și Contul meu	49
10.1. Înregistrarea BitDefender Antivirus 2010	49
10.2. Activarea BitDefender	50
10.3. Achiziționarea unei licențe	53
10.4. Reînnoirea licenței	53
11. Asistenți	54
11.1. Programul asistent de scanare	54
11.1.1. Pasul 1/3 - Scanare	54
11.1.2. Pasul 2/3 - Selectați acțiunile	55
11.1.3. Pasul 3/3 - Examinați rezultatele	57
11.2. Asistent scanare personalizată	58
11.2.1. Pasul 1/6 - Fereastră de întâmpinare	58
11.2.2. Pasul 2/6 - Selectați locația	59
11.2.3. Pasul 3/6 - Selectați acțiunile	61
11.2.4. Pasul 4/6 - Setări suplimentare	63
11.2.5. Pasul 5/6 - Scanare	64
11.2.6. Pasul 6/6 - Examinați rezultatele	65
11.3. Asistent Verificare vulnerabilități	66
11.3.1. Pasul 1/6 - Selectați vulnerabilitățile de verificat	67
11.3.2. Pasul 2/6 - Căutare vulnerabilități	68
11.3.3. Pasul 3/6 - Actualizați Windows	69
11.3.4. Pasul 4/6 - Actualizați aplicații	70
11.3.5. Pasul 5/6 - Schimbați parolele simple	71
11.3.6. Pasul 6/6 - Examinați rezultatele	72
Modul Intermediar	73
12. Pagina de stare	74
13. Antivirus	76
13.1. Zona de stare	76
13.1.1. Configurarea monitorizării stării	77
13.2. Sarcini rapide	78
13.2.1. Actualizarea BitDefender	78
13.2.2. Scanarea cu BitDefender	79
14. Antiphishing	81

14.1. Zona de stare	81
14.2. Sarcini rapide	82
14.2.1. Actualizarea BitDefender	82
14.2.2. Scanarea cu BitDefender	83
15. Vulnerabilitate	85
15.1. Zona de stare	85
15.2. Sarcini rapide	86
16. Rețea	87
16.1. Sarcini rapide	87
16.1.1. Intrarea în rețeaua BitDefender	88
16.1.2. Adăugarea calculatoarelor la rețeaua BitDefender	88
16.1.3. Administrarea rețelei BitDefender	90
16.1.4. Scanarea tuturor calculatoarelor	92
16.1.5. Actualizarea tuturor calculatoarelor	93
16.1.6. Înregistrarea tuturor calculatoarelor	94
Modul Expert	95
17. General	96
17.1. Pagina de stare	96
17.1.1. Stare Generală	97
17.1.2. Statistici	99
17.1.3. Descriere generală	100
17.2. Setări	100
17.2.1. Setări generale	101
17.2.2. Setări raportare viruși	102
17.3. Informații sistem	103
18. Antivirus	105
18.1. Protecție în timp real	105
18.1.1. Configurarea nivelului de protecție	106
18.1.2. Personalizarea nivelului de protecție	107
18.1.3. Configurarea setărilor Active Virus Control	111
18.1.4. Dezactivarea protecției în timp real	114
18.1.5. Configurarea protecției antiphishing	114
18.2. Scanarea la cerere	115
18.2.1. Sarcini de scanare	116
18.2.2. Utilizarea meniului contextual	118
18.2.3. Crearea sarcinilor de scanare	119
18.2.4. Configurarea sarcinilor de scanare	119
18.2.5. Scanarea fișierelor și directoarelor	131
18.2.6. Examinarea rapoartelor de scanare	139
18.3. Obiecte excluse de la scanare	140
18.3.1. Excluderea căilor de la scanare	142
18.3.2. Excluderea extensiilor de la scanare	145
18.4. Zona de carantină	149
18.4.1. Gestionarea fișierelor din carantină	150
18.4.2. Configurarea setărilor carantinei	151

19. Control date	153
19.1. Status Control date	153
19.1.1. Configurarea nivelului de protecție	154
19.2. Control identitate	154
19.2.1. Crearea regulilor de identitate	156
19.2.2. Definirea excepțiilor	159
19.2.3. Administrarea regulilor	161
19.2.4. Regulile stabilite de alți administratori	161
19.3. Control regiștri	162
19.4. Controlul fișierelor cookie	163
19.4.1. Fereastra de configurare	165
19.5. Control scripturi	167
19.5.1. Fereastra de configurare	168
20. Vulnerabilitate	170
20.1. Stare	170
20.1.1. Remedierea vulnerabilităților	171
20.2. Setări	171
21. Criptarea mesageriei instant	173
21.1. Dezactivarea criptării pentru anumiți utilizatori	174
22. Modul pentru jocuri / laptop	176
22.1. Modul pentru jocuri	176
22.1.1. Configurarea modului pentru jocuri automat	177
22.1.2. Administrarea listei de jocuri	178
22.1.3. Configurarea setărilor modului pentru jocuri	179
22.1.4. Schimbarea combinației de taste	179
22.2. Modul pentru laptop	180
22.2.1. Configurarea setărilor modului pentru laptop	181
23. Rețeaua personală	182
23.1. Intrarea în rețeaua BitDefender	182
23.2. Adăugarea calculatoarelor la rețeaua BitDefender	183
23.3. Administrarea rețelei BitDefender	185
24. Actualizare	188
24.1. Actualizarea Automată	188
24.1.1. Cererea unei actualizări	189
24.1.2. Dezactivarea actualizării automate	190
24.2. Setări de Actualizare	190
24.2.1. Configurarea locațiilor de actualizare	191
24.2.2. Configurarea actualizării automate	192
24.2.3. Configurarea actualizării manuale	192
24.2.4. Configurarea setărilor avansate	192
24.2.5. Administrarea proxy-urilor	193
25. Înregistrare	195
25.1. Înregistrarea BitDefender Antivirus 2010	195
25.2. Crearea unui cont BitDefender	196

Integrarea în Windows și în aplicațiile terților	200
26. Integrarea în meniul contextual Windows	201
26.1. Scanează cu BitDefender	201
27. Integrarea cu browserele web	203
28. Integrarea în clienți de mesagerie instant	206
Ghid de instrucțiuni	207
29. Cum scanați fișiere și directoare	208
29.1. Utilizând meniul contextual Windows	208
29.2. Utilizând sarcini de scanare	208
29.3. Utilizând opțiunea Scanare manuală BitDefender	211
29.4. Utilizarea barei de scanare	212
30. Cum să programați scanarea calculatorului	213
Remedierea problemelor și asistența	215
31. Remedierea problemelor	216
31.1. Probleme la instalare	216
31.1.1. Erori de validare a instalării	216
31.1.2. Instalare eșuată	217
31.2. Serviciile BitDefender nu răspund	218
31.3. Nu s-a reușit deinstalarea BitDefender	219
32. Suport	221
32.1. BitDefender Knowledge Base	221
32.2. Solicitarea ajutorului	221
32.3. Informații de contact	222
32.3.1. Adrese Web	222
32.3.2. Filialele BitDefender	222
BitDefender Rescue CD	224
33. Descriere generală	225
33.1. Cerințe de sistem	225
33.2. Soft inclus	226
34. Instrucțiuni BitDefender Rescue CD	229
34.1. Pornirea BitDefender Rescue CD	229
34.2. Oprirea BitDefender Rescue CD	230
34.3. Cum realizez o scanare antivirus?	231
34.4. Cum configurez conexiunea Internet?	232
34.5. Cum actualizez BitDefender?	233
34.5.1. Cum actualizez BitDefender printr-un proxy?	234
34.6. Cum îmi salvez datele?	235
34.7. Cum folosesc modul consolă?	237
Vocabular	238

Contract de licență pentru utilizatorul final

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 SERVICIULI FURNIZAȚE. BITDEFENDER DECLINĂ ÎN MOD EXPLICIT ORICE GARANȚII ȘI CONDIȚII IMPLICITE, INCLUZÂND, FĂRĂ LIMITARE, GARANȚIILE IMPLICITE ALĂ VANDABILITĂȚII, UTILIZĂRII ÎNTR-UN ANUMIT SCOP, TITLULUI, NON-INTERFERENȚEI, ACURATEȚEI DATELOR, A CONȚINUTULUI INFORMAȚIONAL, INTEGRĂRII SISTEMULUI ȘI NEÎNCĂLCĂRII DREPTURILOR UNOR TERȚE PĂRȚI PRIN FILTRAREA, DEZACTIVAREA SAU ÎNDEPĂRTAREA SOFTULUI ACESTORA, A APLICAȚIILOR SPYWARE, ADWARE, A FIȘIERELOR COOKIE, MESAJELOR E-MAIL, DOCUMENTELOR, RECLAMELOR SAU A ALTORA DE GENUL, INDIFERENT DACĂ ACEASTA REIEȘI DIN STATUT, LEGE, FUNCȚIONARE SAU COMERȚ.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

BitDefender Antivirus 2010

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

Prefață

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

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

Vă dorim o lectură plăcută și utilă.

1. Convenții utilizate în manual

1.1. Convenții tipografice

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

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

1.2. Atenționări

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



Notă

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



Important

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



Avertisment

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

2. Structura manualului

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

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

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

Modul Intermediar. Prezintă interfața BitDefender în Modul Intermediar.

Modul Expert. O prezentare detaliată a interfeței BitDefender în Modul Expert. Sunteți învățat cum să configurați și să utilizați toate modulele BitDefender astfel încât să vă protejați eficient calculatorul împotriva oricăror amenințări malițioase (virusi, aplicații spyware, rootkit-uri și altele).

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

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

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

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

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

3. Comentarii

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

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



Important

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

Instalare și dezinstalare

1. Cerințe de sistem

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

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

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



Notă

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

1.1. Cerințe de sistem minime

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

1.2. Cerințe de sistem recomandate

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

1.3. Aplicații în care se poate integra BitDefender

Protecția antiphishing este oferită doar pentru:

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

Criptarea mesageriei instant (IM) este oferită doar pentru:

- Yahoo Messenger 8.5
- Windows Live Messenger 8

2. Pregătirea pentru instalare

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

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

3. Instalarea BitDefender

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

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



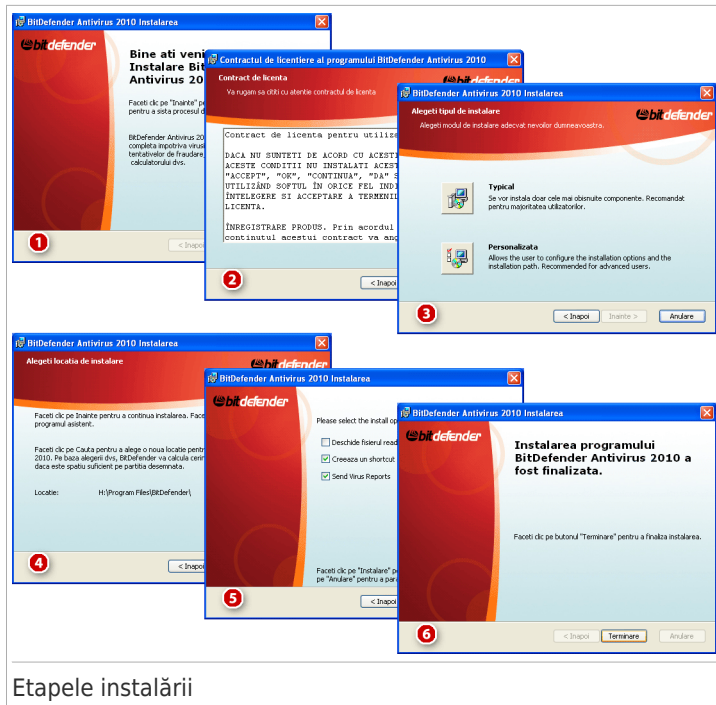
Notă

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

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

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

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



Etapele instalării

Urmați acești pași pentru a instala BitDefender Antivirus 2010:

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

BitDefender Antivirus 2010 vă alertează dacă aveți un alt produs antivirus instalat pe calculatorul dumneavoastră. Faceți clic pe **Șterge** pentru a dezinstala produsul corespunzător. Dacă doriți să continuați fără a dezinstala produsele detectate, faceți clic pe **Înainte**.



Avertisment

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

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



Important

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

3. Selectați tipul de instalare.

- **Tipică** - pentru a instala programul imediat, folosind opțiunile de instalare implicite. Dacă alegeți această opțiune, treceți la pasul 6.
- **Personalizată** - pentru a configura chiar dvs setările de instalare și pentru a instala apoi programul. Această opțiune vă permite să modificați calea de instalare.

4. În mod implicit, BitDefender Antivirus 2010 va fi instalat în C:\Program Files\BitDefender\BitDefender 2010. Dacă doriți să schimbați calea de instalare, faceți clic pe butonul **Caută** și selectați directorul în care doriți să fie instalat BitDefender.

Faceți clic pe **Înainte**.

5. Selectați opțiuni referitoare la procesul de instalare. Opțiunile recomandate sunt selectate implicit:

- **Deschide fișierul readme** - pentru deschiderea fișierului readme la sfârșitul instalării.
- **Creează scurtătură pe desktop** - pentru a crea pe desktop o scurtătură (shortcut) către BitDefender Antivirus 2010 la sfârșitul instalării.
- **Dezactivează cache DNS** - Pentru a dezactiva cache-ul DNS (Domain Name System). Serviciul DNS Client poate fi folosit de aplicațiile periculoase pentru transmiterea de informații în rețea fără permisiunea dvs.
- **Trimite rapoarte de viruși** - Pentru a trimite rapoarte de scanare antivirus la Laboratorul BitDefender pentru analiză. Rapoartele nu conțin date confidențiale, cum ar fi numele dumneavoastră sau adresa IP, și nu vor fi folosite în scopuri comerciale.
- **Dezactivează Windows Defender** - pentru a dezactiva aplicația Windows Defender; această opțiune apare numai pe Windows Vista.

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

6. Așteptați până când instalarea este finalizată și apoi faceți clic pe **Terminare**. Vi se va cere să reporniți sistemul pentru a finaliza procesul de instalare. Faceți acest lucru cât mai curând posibil.



Important

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

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

3.1. Asistentul de înregistrare

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

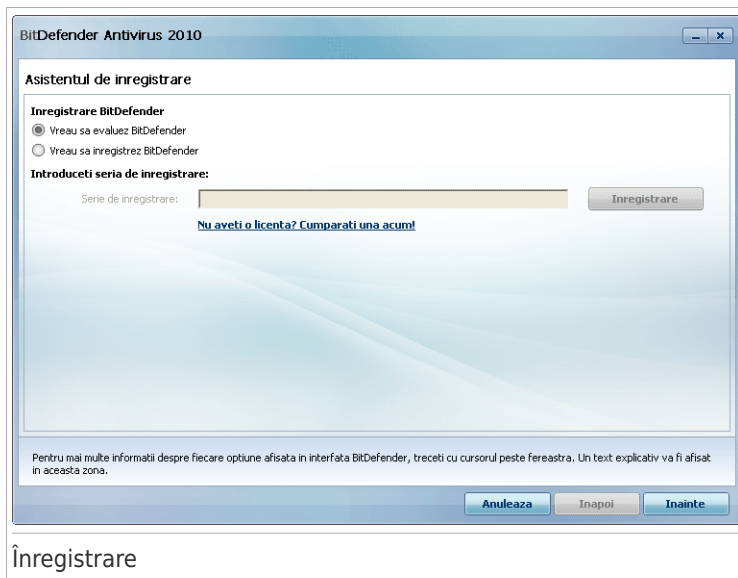
ESTE NECESAR să vă creați un cont BitDefender pentru a primi actualizări BitDefender. Contul BitDefender vă oferă acces la suport tehnic gratuit, oferte speciale și promoții. Dacă v-ați pierdut seria de înregistrare BitDefender, puteți accesa contul dumneavoastră la <http://myaccount.bitdefender.com>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



Notă

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

3.1.1. Pasul 1 - Înregistrați BitDefender Antivirus 2010



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

Pentru a înregistra BitDefender Antivirus 2010:

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



Notă

Puteți găsi seria dumneavoastră de înregistrare:

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

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

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

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

3.1.2. Pasul 2 - Creați un cont BitDefender

Asistentul de inregistrare

Cont BitDefender

Pentru a avea acces la actualizari anti malware si la suport tehnic, activati BitDefender prin crearea/accesarea unui cont. Activarea poate fi amanata 15 zile pentru versiunile de evaluare si 30 de zile pentru versiunile inregistrate. Mai multe informatii la http://www.bitdefender.com/why_register.

Creeaza cont nou

Adresa de e-mail:

Parola: Confirmati parola:

Optiuni e-mail:

Acceseaza cont creat anterior

Amana inregistrarea (inregistrarea este obligatorie)

Pentru mai multe informatii despre fiecare optiune afisata in interfaa BitDefender, treceti cu cursorul peste fereastra. Un text explicativ va fi afisat in aceasta zona.

Creare cont

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

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



Important

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

Nu am un cont BitDefender

Pentru a crea un cont BitDefender, urmați acești pași:

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

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



Notă

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

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

Deja am un cont BitDefender

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

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

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



Notă

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

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

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

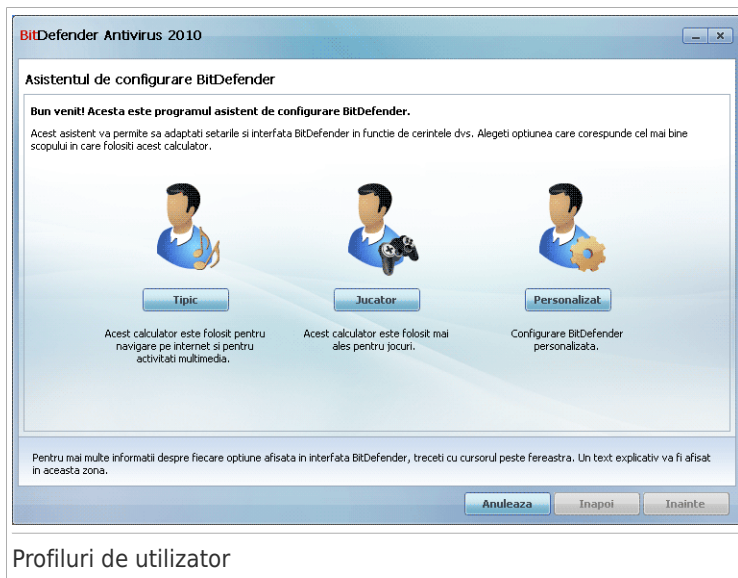
3.2. Asistentul de configurare

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

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

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

3.2.1. Pasul 1 - Selectați profilul de utilizator



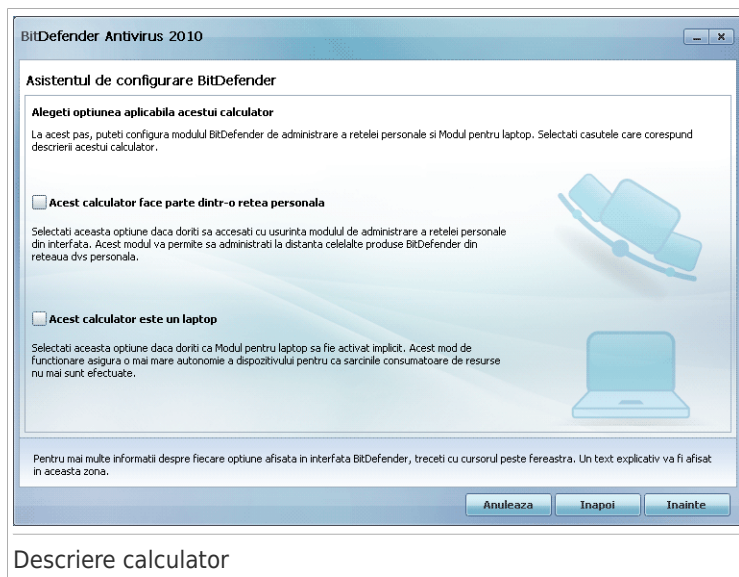
Profiluri de utilizator

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

Opțiune	Descriere
Tipic	Faceți clic aici dacă acest calculator este folosit mai ales pentru navigare și activități multimedia.
Jucător	Faceți clic aici dacă acest calculator este folosit mai ales pentru jocuri.
Personalizat	Faceți clic aici dacă doriți să configurați toate setările principale ale BitDefender.

Puteți reseta profilul de utilizator ulterior, din interfața produsului.

3.2.2. Pasul 2 - Descrieți calculatorul



Selectați opțiunile care se aplică în cazul calculatorului dvs:

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

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

3.2.3. Pasul 3 - Selectați interfața



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

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

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

3.2.4. Pasul 4 - Configurați rețeaua BitDefender



Notă

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

BitDefender Antivirus 2010

Asistentul de configurare BitDefender

Configurarea rețelei personale

BitDefender Antivirus 2010 include modulul de administrare a rețelei personale, care va permite să creați o rețea virtuală a calculatoarelor Familiei dvs și să administrați soluțiile BitDefender instalate pe acestea. Puteți fi administratorul rețelei pe care o creați sau puteți face parte dintr-o rețea creată și administrată de pe un alt calculator.

Activare rețeaua personală

Parola de administrare a rețelei:

Confirmați parola:

Pentru mai multe informații despre fiecare opțiune afișată în interfața BitDefender, treceți cu cursorul peste fereastra. Un text explicativ va fi afișat în această zonă.

Anulează Înapoi Înainte

Configurarea rețelei BitDefender

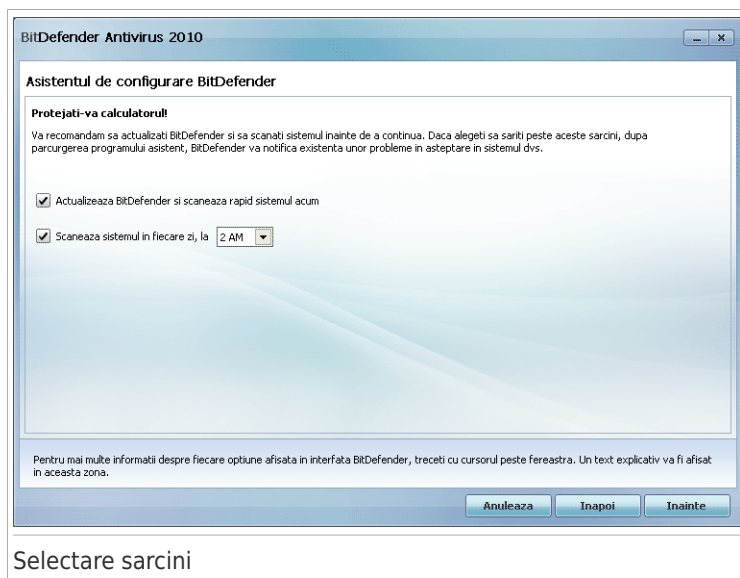
BitDefender vă permite să creați o rețea virtuală a calculatoarelor din locuința dumneavoastră și să administrați produsele BitDefender instalate în această rețea.

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

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

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

3.2.5. Pasul 5 - Selectați sarcinile ce vor fi rulate



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

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

dorită. Dacă aveți calculatorul închis atunci când sarcina trebuie să ruleze, aceasta va fi executată imediat ce deschideți calculatorul.



Notă

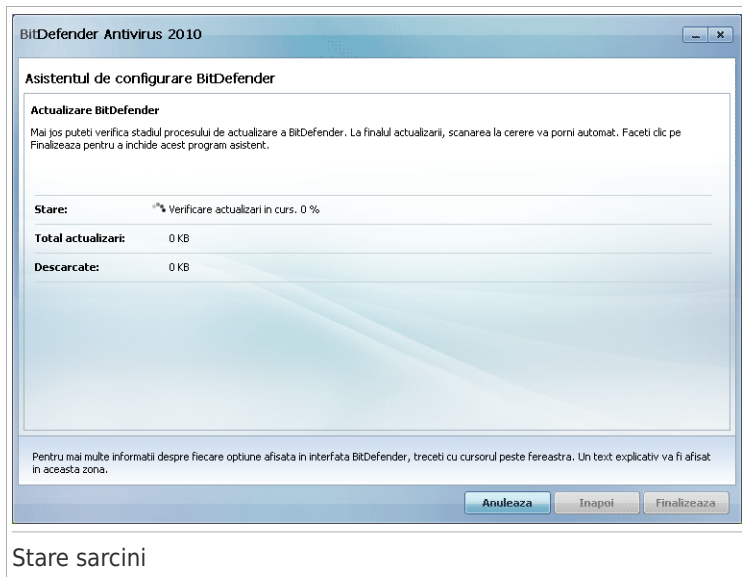
Dacă, mai târziu, doriți să modificați ora la care este programată să ruleze scanarea, urmați acești pași:

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


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

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

3.2.6. Pasul 6 - Finalizare



Așteptați ca BitDefender să-și actualizeze semnăturile de viruși și motoarele de scanare. Imediat ce actualizarea este finalizată, se va porni o scanare rapidă de

sistem. Scanarea va fi efectuată discret, în fundal. Puteți observa iconița de scanare în curs  în **bara de sistem**. Puteți face dublu-clic pe această iconiță pentru a deschide fereastra de scanare și a vedea evoluția scanării.

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



Notă

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

4. Actualizarea versiunii de produs

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

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

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

5. Repararea sau dezinstalarea BitDefender

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

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

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

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

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

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

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



Notă

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

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



Important

Doar pentru Windows Vista! Dezinstalând BitDefender, nu veți mai fi protejat împotriva amenințărilor malițioase, precum virusii și aplicațiile spyware. Dacă doriți activarea Windows Defender după dezinstalarea BitDefender, selectați căsuța corespunzătoare.

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

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



Notă

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


Introdurre

6. Descriere generală

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

Dacă nu ați înregistrat produsul (inclusiv prin crearea unui cont BitDefender), amintiți-vă să faceți acest lucru până la încheierea perioadei de evaluare. Este necesar să vă creați un cont în termen de 15 zile de la instalarea BitDefender (dacă înregistrați produsul cu o serie de înregistrare, termenul limită se extinde la 30 de zile). În caz contrar, BitDefender nu se va mai actualiza. Pentru mai multe informații despre procesul de înregistrare, consultați secțiunea „**Înregistrare și Contul meu**” (p. 49).

6.1. Deschiderea BitDefender

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

6.2. Moduri de vizualizarea a interfeței cu utilizatorul

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


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

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

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

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

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

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

6.2.1. Modul Novice

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



Modul Novice

Fereastra conține patru secțiuni principale:

- **Stare securitate** vă informează dacă sunt probleme care afectează securitatea calculatorului dumneavoastră și vă ajută să le rezolvați. Dacă faceți clic pe **Remediază**, un program asistent vă va permite să eliminați cu ușurință orice pericol la adresa calculatorului și a datelor dvs. Pentru mai multe detalii, consultați *„Remediere probleme”* (p. 38).
- **Protecție calculator** - aici puteți găsi sarcinile necesare pentru a vă proteja calculatorul și datele. Sarcinile disponibile pe care le puteți efectua diferă în funcție de profilul de utilizator selectat.
 - ▶ Butonul **Scanează acum** pornește o scanare standard a sistemului dvs, după viruși, programe spion și alte aplicații periculoase. Va apărea programul asistent Scanare antivirus, care vă va ghida în procesul de scanare. Pentru informații detaliate despre acest program asistent, consultați secțiunea *„Programul asistent de scanare”* (p. 54).
 - ▶ Butonul **Actualizează acum** vă permite să actualizați semnăturile de viruși și fișierele de produs ale BitDefender. Va apărea o nouă fereastră în care puteți vedea starea actualizării. Dacă sunt detectate actualizări, acestea sunt descărcate automat și instalate pe calculatorul dvs.
 - ▶ Când este selectat profilul **Tipic**, butonul **Caută vulnerabilități** pornește un program asistent care vă permite să identificați și să remediați vulnerabilitățile sistemului, cum ar fi: programe neactualizate și actualizări Windows lipsă.

Pentru informații detaliate, consultați secțiunea „*Asistent Verificare vulnerabilități*” (p. 66).

- ▶ La selectarea profilului **Jucător**, butonul **Pornește/oprește Modul pentru jocuri** vă permite să activați/dezactivați **Modul pentru jocuri**. Modul pentru jocuri modifică temporar setările produsului pentru a minimiza impactul acestora asupra performanței sistemului.
- **Întreținere calculator** - aici puteți găsi sarcini suplimentare care vă permit să vă protejați calculatorul și datele.
 - ▶ **Scanare profundă de sistem** - pornește o scanare completă a sistemului dvs, după toate tipurile de programe periculoase.
 - ▶ **Scanare My Documents** - scanează după viruși și alte programe periculoase directoarele dvs cel mai des folosite: My Documents și Desktop. Astfel, documentele dvs sunt protejate, iar spațiul de lucru și aplicațiile care rulează la pornirea sistemului sunt sigure.
 - ▶ **Scanare autologon** scanează obiectele care sunt rulate atunci când deschideți sesiunea Windows.
- **Profil utilizator** indică profilul de utilizator selectat. Profilul utilizatorului reflectă principalele activități desfășurate pe calculator. În funcție de profil, interfața produsului este organizată astfel încât să vă permită să accesați ușor sarcinile dvs favorite.

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

În colțul din dreapta, sus al ferestrei, se află butonul **Setări**. Acesta deschide o fereastră în care puteți schimba modul de vizualizare a interfeței cu utilizatorul sau dezactiva setările principale ale BitDefender. Pentru mai multe detalii, consultați „*Configurarea setărilor de bază*” (p. 42).

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

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

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

6.2.2. Modul Intermediar

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



Fereastra Mod intermediar conține cinci taburi. Tabelul de mai jos conține o scurtă descriere a fiecărui tab. Pentru mai multe detalii, consultați secțiunea „Modul Intermediar” (p. 73) a acestui manual.

Tab	Descriere
Stare	Afișează starea de securitate a sistemului dvs și vă permite să resetați profilul de utilizator.
Antivirus	Afișează starea modulului antivirus care vă ajută să actualizați BitDefender și să vă protejați sistemul de viruși.

Tab	Descriere
Antiphishing	Afișează starea modulelor care vă protejează împotriva furtului de informații personale (phishing) atunci când sunteți online.
Vulnerabilitate	Afișează starea modulului vulnerabilitate care vă ajută să mențineți actualizate cele mai importante aplicații de pe calculatorul dumneavoastră. Aici puteți remedia cu ușurință orice vulnerabilitate care ar putea afecta securitatea calculatorului dumneavoastră.
Rețea	Afișează structura rețelei BitDefender. Aici puteți efectua diverse acțiuni pentru a configura și administra produsele BitDefender instalate în rețeaua dumneavoastră personală. În acest fel, puteți administra securitatea rețelei dumneavoastră personale de la un singur calculator.

În colțul din dreapta, sus al ferestrei, se află butonul **Setări**. Acesta deschide o fereastră în care puteți schimba modul de vizualizare a interfeței cu utilizatorul sau dezactiva setările principale ale BitDefender. Pentru mai multe detalii, consultați „*Configurarea setărilor de bază*” (p. 42).

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

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

6.2.3. Modul Expert

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



Notă

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

Modul Stare afișează starea de securitate a produsului dvs și linkuri către cele mai importante module ale produsului dvs.

Modul Expert

În partea stângă a ferestrei există un meniu care conține toate modulele de securitate. Fiecare modul are unul sau mai multe taburi în care puteți configura setările de securitate corespunzătoare sau puteți efectua sarcini de securitate/administrative. Tabelul următor conține o scurtă descriere a fiecărui tab. Pentru mai multe detalii, consultați secțiunea „Modul Expert” (p. 95) a acestui manual.

Modul	Descriere
General	Vă permite să accesați setările generale sau să vizualizați pagina de stare și informații detaliate despre sistem.
Antivirus	Vă permite să configurați scutul antivirus și operațiile de scanare în detaliu, să setați excepții și să configurați modulul de carantină.

Modul	Descriere
Control date	Vă permite să preveniți furtul de date de pe calculatorul dumneavoastră și să vă protejați confidențialitatea în timp ce sunteți online.
Vulnerabilitate	Vă permite să mențineți actualizate cele mai importante aplicații de pe calculatorul dumneavoastră.
Criptare	Vă permite să criptați comunicațiile prin Yahoo și Windows Live (MSN) Messenger.
Mod jocuri/laptop	Vă permite să amânați executarea sarcinilor BitDefender programate cât timp laptopul dumneavoastră funcționează pe baterii și, de asemenea, să eliminați toate alertele și pop-upurile atunci când vă jucați pe calculator.
Rețea	Vă permite să configurați și să administrați mai multe calculatoare din locuința dumneavoastră.
Actualizare	Vă permite să obțineți informații despre cele mai recente actualizări, să actualizați produsul și să configurați procesul de actualizare în detaliu.
Înregistrare	Vă permite să înregistrați BitDefender Antivirus 2010, să schimbați seria de înregistrare sau să creați un cont BitDefender.

În colțul din dreapta, sus al ferestrei, se află butonul **Setări**. Acesta deschide o fereastră în care puteți schimba modul de vizualizare a interfeței cu utilizatorul sau dezactiva setările principale ale BitDefender. Pentru mai multe detalii, consultați „*Configurarea setărilor de bază*” (p. 42).

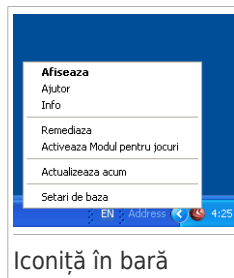
În colțul din dreapta, jos al ferestrei, puteți găsi mai multe link-uri utile.

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

6.3. Iconiță în bara de sistem

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

- **Afișează** - deschide interfața principală a BitDefender.
- **Ajutor** - deschide documentația electronică, unde vi se explică în detaliu cum să configurați și să utilizați produsul BitDefender Antivirus 2010.
- **Despre** - deschide o fereastră în care puteți vedea informații despre BitDefender și unde să apălați pentru ajutor în cazul unei probleme.
- **Remediază** - vă ajută să remediați problemele curente de securitate. Dacă opțiunea nu este disponibilă, nu există probleme care trebuie remediate. Pentru mai multe detalii, consultați „*Remediere probleme*” (p. 38).
- **Activează/Dezactivează Modul pentru jocuri** - activează/dezactivează **modul pentru jocuri**.
- **Actualizează acum** - inițiază o actualizare imediată. Va apărea o nouă fereastră în care puteți vedea starea actualizării.
- **Setări de bază** - deschide o fereastră în care puteți schimba modul de vizualizare a interfeței cu utilizatorul și să activați sau să dezactivați setările principale ale produsului. Pentru mai multe informații, consultați secțiunea „*Configurarea setărilor de bază*” (p. 42).



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

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

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

6.4. Bara de scanare

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

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



Notă

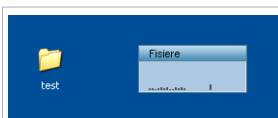
Bara de scanare vă va avertiza când protecția în timp real este dezactivată prin afișarea unui X roșu deasupra zonei **Fișiere**.



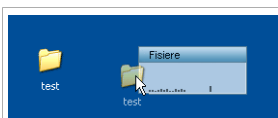
Bara de scanare

6.4.1. Scanare fișiere și directoare

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



Trageți fișierul



Lăsați fișierul

Va apărea programul asistent Scanare antivirus, care vă va ghida în procesul de scanare. Pentru informații detaliate despre acest program asistent, consultați secțiunea „*Programul asistent de scanare*” (p. 54).

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

6.4.2. Dezactivarea/Reactivarea barei de scanare

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

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

6.5. Scanare manuală BitDefender

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

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



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

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

După ce ați terminat de selectat locațiile, faceți clic pe **Continuă**. Va apărea programul asistent Scanare antivirus, care vă va ghida în procesul de scanare. Pentru informații detaliate despre acest program asistent, consultați secțiunea „*Programul asistent de scanare*” (p. 54).

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

Ce este Safe Mode?

Safe Mode este un mod special de a porni Windows, utilizat în principal pentru a depana problemele care afectează funcționarea normală a Windows. Aceste probleme variază de la conflicte provocate de drivere până la viruși care împiedică pornirea normală a Windows. În Safe Mode, Windows încarcă doar un minim de componente ale sistemului de operare și drivere de bază. Doar câteva aplicații funcționează în Safe Mode. Acesta este motivul pentru care majoritatea virușilor sunt inactivi și pot fi ușor eliminați atunci când Windows operează în Safe Mode.

Pentru a porni Windows în Safe Mode, reporniți calculatorul și apăsați tasta F8 încontinuu până apare meniul de opțiuni avansate al Windows (Windows Advanced Options Menu). Puteți alege între mai multe opțiuni de a porni Windows în Safe Mode. Este recomandat să selectați **Safe Mode with Networking** pentru a avea acces la Internet.



Notă

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

6.6. Modul pentru jocuri și Modul pentru laptop

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


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

- Modul pentru jocuri
- Modul pentru laptop

6.6.1. Modul pentru jocuri

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

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

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

Utilizarea modului pentru jocuri

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

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

- Faceți clic-dreapta pe icoana BitDefender din bara de sistem și selectați **Activează modul pentru jocuri**.
- Apăsați simultan tastele **Ct r l+Sh i ft+Al t+G** (combinația de taste implicită).



Important

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

Schimbarea combinației de taste

Pentru a schimba combinația de taste, urmați acești pași:

1. Deschideți BitDefender și treceți interfața în Modul Expert.
2. Faceți clic pe **Mod jocuri/laptop** în meniul din stânga.
3. Faceți clic pe tabul **Mod jocuri**
4. Faceți clic pe butonul **Setări avansate**.

5. Sub opțiunea **Utilizează combinația de taste**, setați combinația de taste dorită:

- Bifați tastele speciale pe care doriți să le folosiți: tasta Control (Ct r l), tasta Shift (Sh i f t) sau tasta Alternate (A l t).
- În câmpul editabil, tastați litera corespunzătoare tastei normale pe care doriți să o folosiți.

De exemplu, dacă doriți să folosiți combinația de taste Ct r l+A l t+D, trebuie să bifați doar Ct r l și A l t și să tastați D.



Notă

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

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

6.6.2. Modul pentru laptop

Modul pentru laptop este creat special pentru utilizatorii de laptopuri. Scopul acestuia este să minimizeze impactul pe care îl are BitDefender asupra consumului bateriei atunci când aceste dispozitive funcționează pe baterie. Dacă este activat Modul pentru laptop, sarcinile de scanare programate nu sunt efectuate atunci când laptopul se alimentează de la baterie deoarece acestea necesită mai multe resurse de sistem și sporesc, implicit, consumul de energie.

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

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

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

6.7. Detectie automată unități

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

Unitățile detectate fac parte din următoarele categorii:

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

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

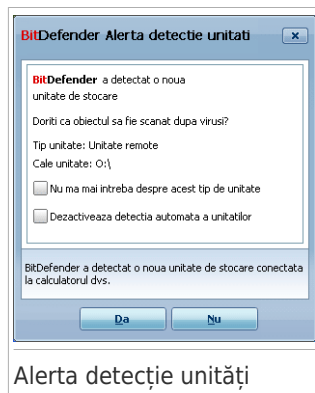
Pentru a scana unitatea de stocare, faceți clic pe **Da**. Va apărea programul asistent Scanare antivirus, care vă va ghida în procesul de scanare. Pentru informații detaliate despre acest program asistent, consultați secțiunea „*Programul asistent de scanare*” (p. 54).

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

- **Nu mă mai întreba despre acest tip de unitate** - BitDefender nu va mai propune scanarea unităților de stocare de acest tip atunci când acestea sunt conectate la calculator.
- **Dezactivează detecția automată a unităților** - Nu vi se va mai propune să scanați noile unități de stocare atunci când acestea sunt conectate la calculator.

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

1. Deschideți BitDefender și treceți interfața în Modul Expert.
2. Mergeți la **Antivirus>Scanare viruși**.
3. În lista de sarcini de scanare, localizați sarcina **Scanare detecție unități**.
4. Faceți clic-dreapta pe sarcină și selectați **Deschidere**. Va apărea o nouă fereastră.
5. Pe tabul **General**, configurați opțiunile de scanare după cum este necesar. Pentru mai multe informații, consultați secțiunea „*Configurarea setărilor de scanare*” (p. 120).
6. Pe tabul **Detecție**, alegeți tipurile de unități de stocare de detectat.
7. Faceți clic pe **OK** pentru a salva și aplica modificările.



7. Remediere probleme

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

Problemele în așteptare sunt semnalate astfel:

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


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

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

- Când deschideți BitDefender, zona de stare a securității va indica numărul de probleme care afectează sistemul dvs.
 - ▶ În Modul Intermediar, starea de securitate este afișată în tabul **Pagina de stare**.
 - ▶ În Modul Expert, mergeți la **General>Pagina de stare** pentru a verifica starea de securitate.

7.1. Asistent Remediere toate problemele

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

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



Asistent Remediere toate problemele

Programul asistent afișează lista vulnerabilităților legate de securitatea calculatorului dvs.

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



Notă

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

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

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

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

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

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

- **Vulnerabilități ale sistemului.** BitDefender verifică automat dacă există vulnerabilități ale sistemului dvs și vă informează în legătură cu acestea. În categoria vulnerabilităților sistemului intră:

- ▶ parolele simple ale conturilor de utilizator Windows.
- ▶ programele neactualizate de pe calculatorul dvs.
- ▶ actualizări Windows lipsă.
- ▶ actualizările Windows automate dezactivate.

Când apar astfel de probleme, se lansează programul asistent de scanare după vulnerabilități. Acesta vă permite să remediați vulnerabilitățile sistemului care au fost detectate. Pentru informații detaliate, consultați secțiunea „*Asistent Verificare vulnerabilități*” (p. 66).

7.2. Configurarea monitorizării problemelor

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

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

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


Pentru mai multe detalii, consultați secțiunea „*Modul Intermediar*” (p. 73) a acestui manual.

- În Modul Expert, sistemul de monitorizare poate fi configurat dintr-o singură locație. Urmați pașii:
 1. Mergeți la **General>Stare**.
 2. Faceți clic pe **Configurare monitorizare stare**.
 3. Selectați căsuțele corespunzătoare obiectelor care doriți să fie monitorizate.

Pentru informații detaliate, consultați capitolul „*Pagina de stare*” (p. 96).

8. Configurarea setărilor de bază

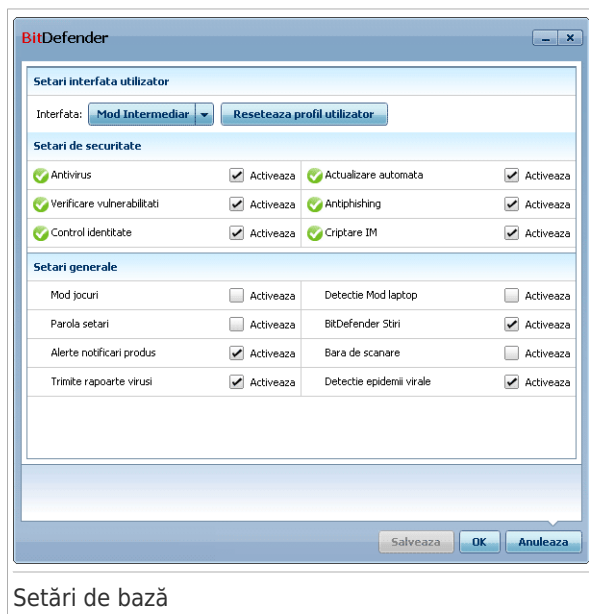
Puteți să configurați setările principale de produs (inclusiv să schimbați modul de vizualizare a interfeței cu utilizatorul) din fereastra de setări de bază. Pentru a o deschide, aveți următoarele opțiuni:

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



Notă

Pentru configurarea detaliată a setărilor de produs, folosiți interfața în Modul Expert. Pentru mai multe detalii, consultați secțiunea „Modul Expert” (p. 95) a acestui manual.



Setări de bază

Setările sunt grupate în trei categorii:


- **Setări interfață cu utilizatorul**
- **Setări securitate**
- **Setări generale**

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

8.1. Setări interfață cu utilizatorul

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

Schimbarea modului de vizualizare a interfeței cu utilizatorul. . Conform descrierii din secțiunea „*Moduri de vizualizarea a interfeței cu utilizatorul*” (p. 23), există trei moduri de afișare a interfeței cu utilizatorul. Fiecare mod este destinat unei anumite categorii de utilizatori, în funcție de aptitudinile lor de operare a calculatorului. Astfel, interfața cu utilizatorul corespunde nevoilor tuturor tipurilor de utilizatori, de la începători la experți în utilizarea calculatorului.

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

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

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

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

8.2. Setări de securitate

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

 **Cerc verde cu bifă:** Setarea este activată.

 **Cerc roșu cu semnul exclamării:** Setarea este dezactivată.

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



Avertisment

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

Tabelul următor conține întreaga listă de setări și descrierea lor:

Setare	Descriere
Antivirus	Protecția în timp real asigură scanarea tuturor fișierelor accesate de dvs sau de o aplicație care rulează pe acest sistem.
Actualizare automată	Actualizarea automată asigură descărcarea și instalarea automată, în mod regulat, a celor mai recente fișiere de produs și semnături BitDefender.
Verificare vulnerabilități	Verificarea automată a vulnerabilităților asigură menținerea la zi a aplicațiilor critice de pe calculatorul dumneavoastră.
Antiphishing	Protecția antiphishing detectează și vă alertează în timp real dacă o pagină web este folosită pentru furt de informații personale.
Control identitate	Controlul identității vă permite să împiedicați trimiterea de date cu caracter personal pe Internet, fără consimțământul dvs. Această opțiune blochează orice mesaj instant, e-mail sau formular web prin care se

Setare	Descriere
	transmit către destinatari neautorizați (adrese) date pe care le-ați identificat ca având caracter personal.
Criptare IM	Criptarea mesageriei instant asigură confidențialitatea conversațiilor dvs prin Yahoo! Messenger și Windows Live Messenger cu interlocutori care folosesc un produs BitDefender și o aplicație de mesagerie instant compatibile.

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

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

- În Modul Intermediar, sistemul de monitorizare poate fi configurat din locații diferite, în funcție de categoriile de setări. Pentru mai multe detalii, consultați secțiunea „*Modul Intermediar*” (p. 73) a acestui manual.
- În Modul Expert, sistemul de monitorizare poate fi configurat dintr-o singură locație. Urmați pașii:
 1. Mergeți la **General>Stare**.
 2. Faceți clic pe **Configurare monitorizare stare**.
 3. Deselectați căsuța corespunzătoare obiectului care nu doriți să fie monitorizat.

Pentru informații detaliate, consultați capitolul „*Pagina de stare*” (p. 96).

8.3. Setări generale

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

Tabelul următor conține întreaga listă de setări și descrierea lor:

Setare	Descriere
Mod pentru jocuri	Modul pentru jocuri modifică temporar setările de protecție pentru a minimiza impactul acestora asupra performanței sistemului atunci când vă jucați pe calculator.
Detecție mod pentru laptop	Modul pentru laptop modifică temporar setările de protecție pentru a minimiza impactul acestora asupra duratei de funcționare a laptopului pe baterie.

Setare	Descriere
Parola pentru setări	<p>Aceasta asigură că setările BitDefender pot fi modificate doar de către persoanele care cunosc această parolă.</p> <p>La activarea acestei opțiuni, vi se va cere să configurați parola de setări. Introduceți parola dorită în ambele câmpuri și faceți clic pe OK pentru a o seta.</p>
Știri BitDefender	Activând această opțiune, veți primi știri importante legate de companie, actualizări de produs sau noi amenințări de securitate de la BitDefender.
Alerte de notificare produs	Activând această opțiune, veți primi alerte informative.
Bara de scanare	Bara de scanare este o fereastră mică, transparentă care indică progresul activității de scanare a BitDefender. Pentru mai multe informații, consultați secțiunea „ <i>Bara de scanare</i> ” (p. 32).
Trimite rapoarte viruși	Activând această opțiune, BitDefender va trimite rapoartele de scanare către Laboratorul BitDefender pentru analiză. Aceste rapoarte nu vor conține date confidențiale, cum ar fi numele dumneavoastră sau adresa IP și nu vor fi folosite în scop comercial.
Detecție epidemii virale	Activând această opțiune, BitDefender va trimite rapoarte privind potențiale epidemii virale către Laboratorul BitDefender pentru analiză. Aceste rapoarte nu vor conține date confidențiale, cum ar fi numele dumneavoastră sau adresa IP, și nu vor fi folosite în scop comercial.

9. Istoric și evenimente

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

BitDefender Antivirus 2010

Istoric & Evenimente

Antivirus

- Control date
- Vulnerabilitati
- Criptare IM
- Mod jocuri/laptop
- Rețea personală
- Actualizare
- Inregistrare

Protectie in timp real

Nume actiune	Actiune aplicata	Data
Protectie in timp real	Activat	8/24/2009 3:47:55 PM
Protectie in timp real	Dezactivat	8/24/2009 3:46:33 PM
Protectie in timp real	Activat	8/24/2009 3:40:13 PM
Protectie in timp real	Dezactivat	8/24/2009 3:40:10 PM
Scannerul Comportamental ...	Aplicatia a fost oprita.	8/24/2009 3:40:01 PM

Sarcini la cerere

Nume actiune	Nume sarcina:	Data
Sarcina de scanare finalizata.	4646	8/24/2009 3:47:11 PM
Sarcina de scanare finalizata.	Sarcina de scanare	8/24/2009 3:46:19 PM
Sarcina de scanare abando...	Scanare obiecte excluse	8/24/2009 3:41:52 PM
Sarcina de scanare intrerup...	Scanare in profunzime	8/24/2009 3:40:34 PM
Sarcina de scanare abando...	Scanare rapida sistem	8/24/2009 3:38:46 PM

Pentru mai multe informatii despre fiecare optiune afisata in interfața BitDefender, treceti cu cursorul peste fereastra. Un text explicativ va fi afisat in aceasta zona.

bitdefender

Sterge jurnalele Actualizeaza OK

Evenimente

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

- **Antivirus**
- **Control date**
- **Vulnerabilitate**
- **Criptare IM**
- **Mod jocuri/laptop**
- **Rețea personală**
- **Actualizare**
- **Inregistrare**

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

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

10. Înregistrare și Contul meu

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

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

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



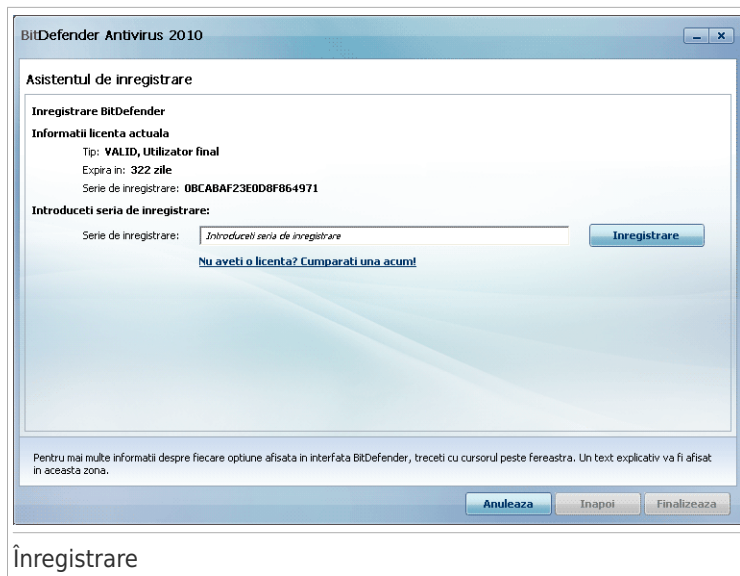
Important

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

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

10.1. Înregistrarea BitDefender Antivirus 2010

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



Înregistrare

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

Pentru a înregistra BitDefender Antivirus 2010:

1. Introduceți seria de înregistrare în câmpul editabil.



Notă

Puteți găsi seria dumneavoastră de înregistrare:

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

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

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

10.2. Activarea BitDefender

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

- În Modul Novice, faceți clic pe **Remediază**. Asistentul vă va permite să remediați toate problemele în așteptare, inclusiv activarea produsului.
- În Modul Intermediar, mergeți la tabul **Securitate** și faceți clic pe butonul **Remediază** corespunzător problemei legate de activarea produsului.
- În Modul Expert, mergeți la **Înregistrare** și faceți clic pe butonul **Activare produs**. Se va deschide fereastra de înregistrare a contului. Aici puteți crea sau vă puteți conecta la un cont BitDefender pentru a vă activa produsul.

BitDefender Antivirus 2010

Asistentul de înregistrare

Cont BitDefender

Pentru a avea acces la actualizările anti-malware și la suport tehnic, activați BitDefender prin crearea/accesarea unui cont. Activarea poate fi amânată 15 zile pentru versiunile de evaluare și 30 de zile pentru versiunile înregistrate. Mai multe informații la http://www.bitdefender.com/why_register.

Creează cont nou

Adresa de e-mail:

Parola: Confirmați parola:

Optiuni e-mail:

Accesează cont creat anterior

Amână înregistrarea (înregistrarea este obligatorie)

Pentru mai multe informații despre fiecare opțiune afișată în interfața BitDefender, treceți cu cursorul peste fereastra. Un text explicativ va fi afișat în această zonă.

Creare cont

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

- „Nu am un cont BitDefender” (p. 51)
- „Deja am un cont BitDefender” (p. 52)



Important

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

Nu am un cont BitDefender

Pentru a crea un cont BitDefender, urmați acești pași:

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



Notă

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

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

Deja am un cont BitDefender

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

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

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



Notă

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

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

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

4. Faceți clic pe **Accesează**.

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

10.3. Achiziționarea unei licențe

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

10.4. Reînnoirea licenței

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

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

11. Asistenți


Pentru a putea folosi BitDefender foarte ușor, aveți la dispoziție o serie de programe asistent care vă permit să efectuați anumite sarcini de securitate sau să configurați setări de produs complexe. Acest capitol conține o descriere a programelor asistent care pot apărea atunci când remediați probleme sau efectuați sarcini specifice cu BitDefender. Alte programe asistent de configurare sunt descrise separat, în secțiunea „Modul Expert” (p. 95).

11.1. Programul asistent de scanare

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

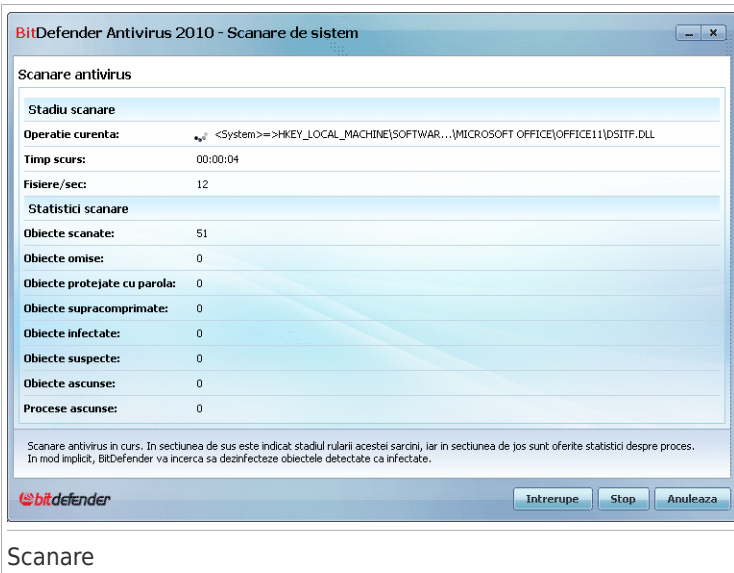


Notă

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

11.1.1. Pasul 1/3 - Scanare

BitDefender va începe scanarea obiectelor selectate.



BitDefender Antivirus 2010 - Scanare de sistem

Scanare antivirus

Stadiu scanare

Operatie curenta: <System>=>HKEY_LOCAL_MACHINE\SOFTWARE...\MICROSOFT OFFICE\OFFICE11\DSITF.DLL

Timp scurs: 00:00:04

Fisiere/sec: 12

Statistici scanare

Obiecte scanate:	51
Obiecte omise:	0
Obiecte protejate cu parola:	0
Obiecte supracompimate:	0
Obiecte infectate:	0
Obiecte suspecte:	0
Obiecte ascunse:	0
Procese ascunse:	0

Scanare antivirus in curs. In sectiunea de sus este indicat stadiul rularii acestei sarcini, iar in sectiunea de jos sunt oferite statistici despre proces. In mod implicit, BitDefender va incerca sa dezinfecteze obiectele detectate ca infectate.

bitdefender [Intrerupe] [Stop] [Anuleaza]

Scanare

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

Așteptați ca BitDefender să finalizeze scanarea.



Notă

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

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

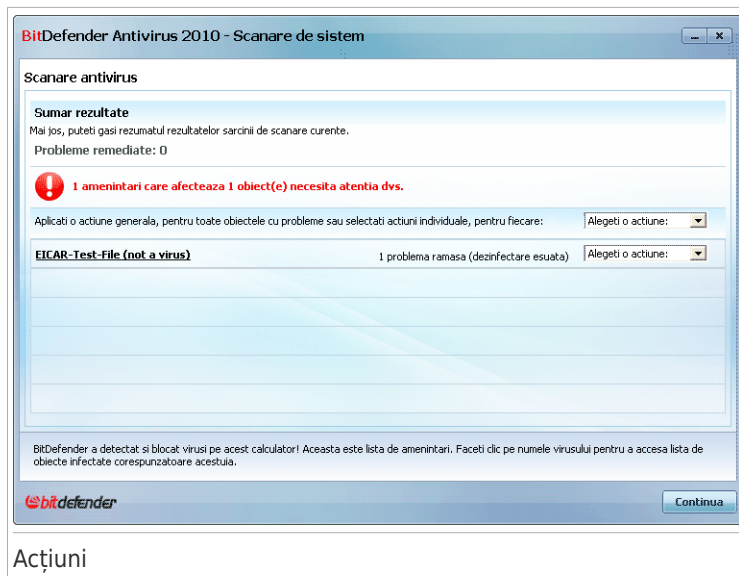
- **Doresc să introduc parola pentru acest obiect.** Dacă doriți ca BitDefender să scaneze arhiva, selectați această opțiune și introduceți parola. Dacă nu cunoașteți parola, selectați una dintre celelalte opțiuni.
- **Nu vreau să introduc parola pentru acest obiect (nu scana acest obiect).** Selectând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

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

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

11.1.2. Pasul 2/3 - Selectați acțiunile

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



Acțiuni

Puteți vedea numărul problemelor care vă afectează sistemul.

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

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

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

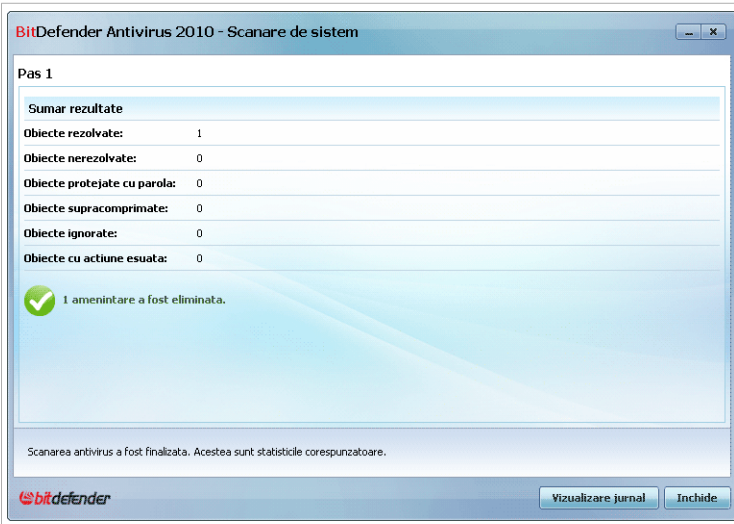
Acțiune	Descriere
Nicio acțiune	Nu se va lua nicio acțiune asupra fișierelor detectate. După finalizarea scanării, puteți deschide raportul de scanare pentru a vedea informații despre aceste fișiere.
Dezinfectează	Elimină codul malițios din fișierele infectate.
Șterge	Șterge fișierele detectate.
Mută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

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

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

11.1.3. Pasul 3/3 - Examinați rezultatele

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



The screenshot shows a window titled "BitDefender Antivirus 2010 - Scanare de sistem". It displays the results of a system scan under "Pas 1". A table summarizes the results:

Sumar rezultate	
Obiecte rezolvate:	1
Obiecte nerezolvate:	0
Obiecte protejate cu parola:	0
Obiecte supracomprimate:	0
Obiecte ignorate:	0
Obiecte cu actiune esuata:	0

Below the table, a green checkmark icon is next to the text "1 amenintare a fost eliminata." At the bottom of the window, there is a message: "Scanarea antivirus a fost finalizata. Acestea sunt statisticele corespunzatoare." and two buttons: "Vizualizare jurnal" and "Inchide".

Rezumat

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



Important

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

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

BitDefender nu a putut remedia anumite probleme

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

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

BitDefender a detectat fișiere suspecte

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

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

11.2. Asistent scanare personalizată

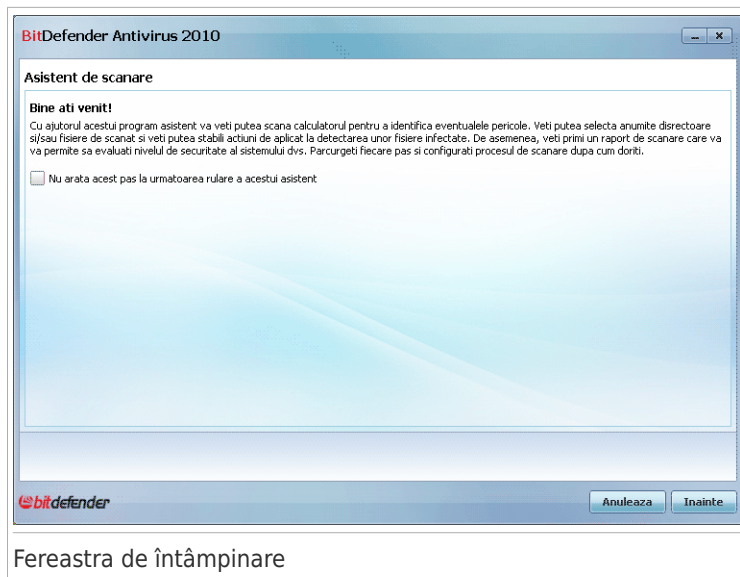
Asistentul de scanare personalizată vă permite să creați și să rulați o sarcină de scanare la cerere și, opțional, s-o salvați ca Sarcină rapidă accesibilă atunci când folosiți BitDefender în Modul Intermediar.

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

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

11.2.1. Pasul 1/6 - Fereastră de întâmpinare

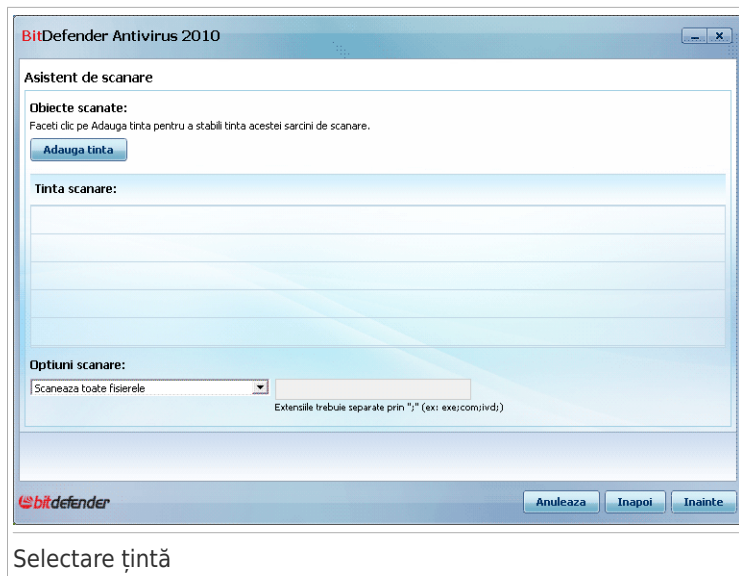
Bine ați venit!



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

11.2.2. Pasul 2/6 - Selectați locația

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



Selectare țintă

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

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

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

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

Faceți clic pe **Înainte**.

11.2.3. Pasul 3/6 - Selectați acțiunile

Aici puteți indica setările și nivelul de scanare.

Asistent de scanare

Acțiuni posibile
 Selectați setările scannerului și stabiliți nivelul de scanare.

Acțiuni pentru fișierele infectate:

Prima acțiune: Dezinfecteaza

A doua acțiune: Nicio acțiune

Acțiuni pentru fișierele suspecte:

Prima acțiune: Nicio acțiune

A doua acțiune: Nicio acțiune

Acțiuni pentru fișierele ascunse (rootkit):

Acțiune: Nicio acțiune

Nivel de scanare
 Selectați nivelul de agresivitate al scannerului mutând cursorul la punctul dorit.

Agresiv Nivel implicit

Implicit - Implicit, consum moderat de resurse
 - Scaneaza fisiere

Permisiv - Scaneaza dupa virusi si spyware

Personalizat

Anuleaza Inapoi Inainte

Selectare acțiuni

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

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

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

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

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

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

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

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

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

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

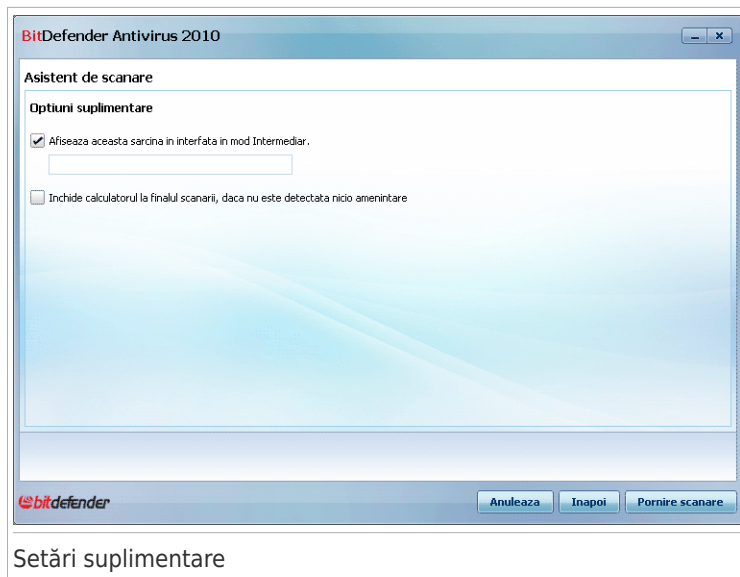
Opțiune	Descriere
Scanează după viruși	Scanează după viruși cunoscuți. BitDefender detectează, de asemenea, și corpurile incomplete de viruși, îndepărtând astfel orice posibilă amenințare ce ar putea afecta securitatea sistemului dumneavoastră.
Scanează după adware	Scanează după amenințări adware. Fișierele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

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

Faceți clic pe **Înainte**.

11.2.4. Pasul 4/6 - Setări suplimentare

Înainte de începutul scanării, sunt disponibile opțiuni suplimentare:



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

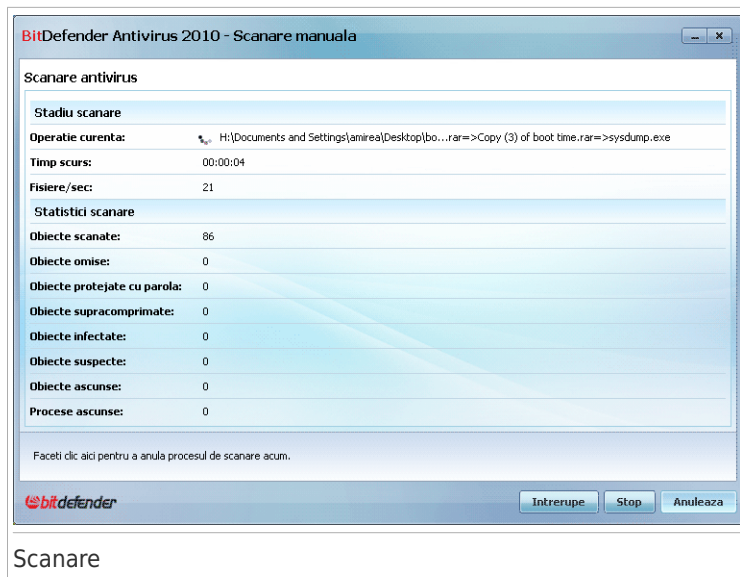
Sarcina va fi adăugată pe lista de Sarcini rapide deja existentă în tabul Securitate și va apărea, de asemenea, în **Modul expert > Antivirus > Scanare viruși**.

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

Faceți clic pe **Pornire scanare**.

11.2.5. Pasul 5/6 - Scanare

BitDefender va începe scanarea obiectelor selectate:

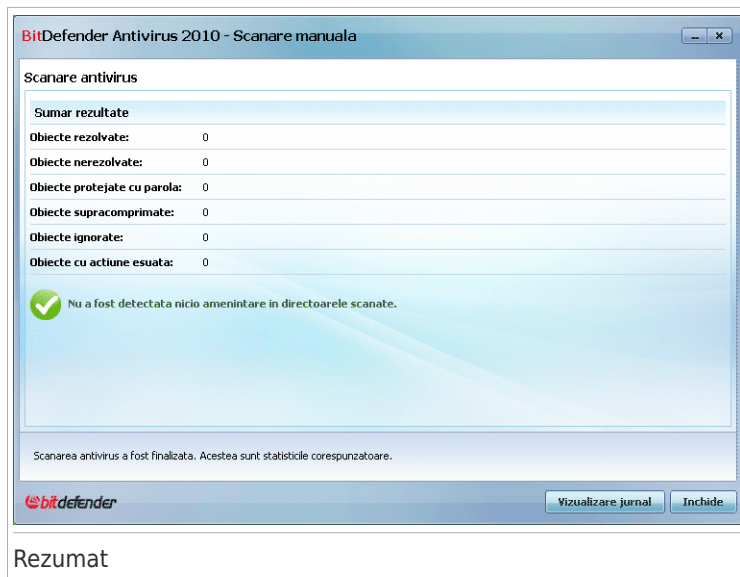


Notă

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

11.2.6. Pasul 6/6 - Examinați rezultatele

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



Rezumat

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



Important

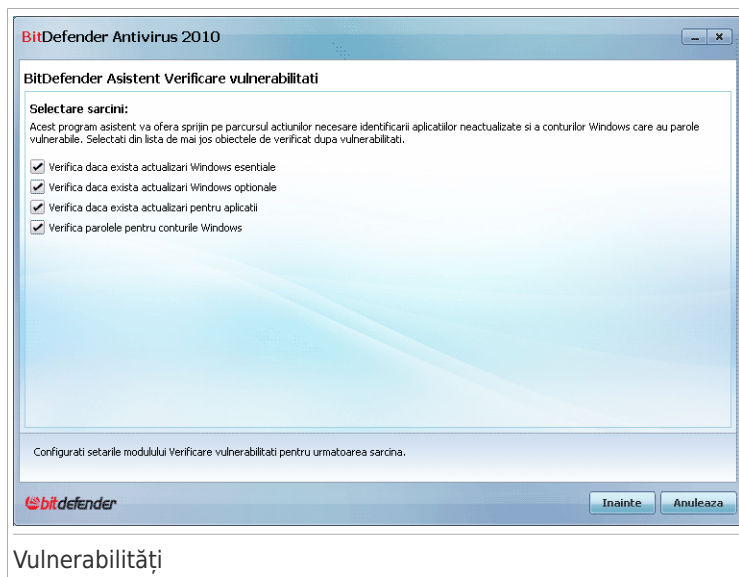
Dacă este necesar, reporniți sistemul pentru a finaliza procesul de curățare.

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

11.3. Asistent Verificare vulnerabilități

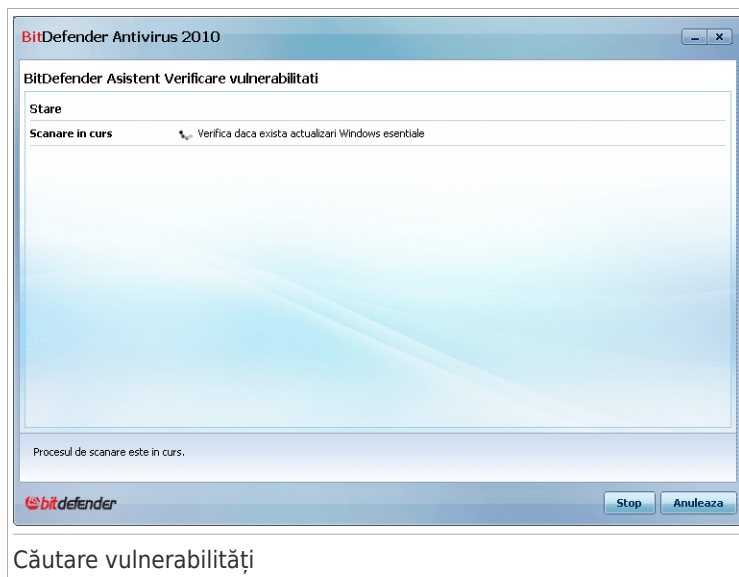
Acest program asistent verifică dacă există vulnerabilități ale sistemului și vă ajută să le remediați.

11.3.1. Pasul 1/6 - Selectați vulnerabilitățile de verificat



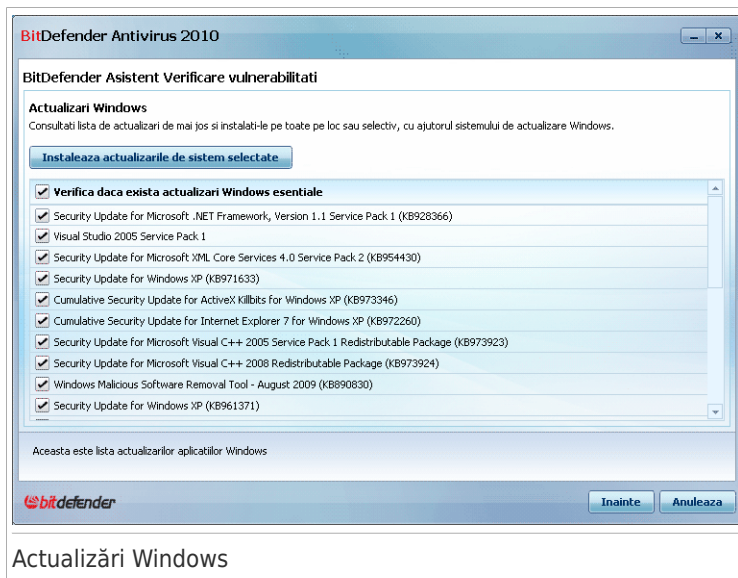
Faceți clic pe **Înainte** pentru a verifica sistemul după vulnerabilitățile selectate.

11.3.2. Pasul 2/6 - Căutare vulnerabilități



Așteptați ca BitDefender să finalizeze căutarea.

11.3.3. Pasul 3/6 - Actualizați Windows



Actualizări Windows

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

Faceți clic pe **Înainte**.

11.3.4. Pasul 4/6 - Actualizați aplicații



The screenshot shows the BitDefender Antivirus 2010 interface for checking application updates. The window title is 'BitDefender Antivirus 2010' and the main heading is 'BitDefender Asistent Verificare vulnerabilitati'. Below the heading is the instruction 'Verifica daca exista actualizari pentru aplicatii'. A table lists three applications: Yahoo! Messenger, Firefox, and Windows Live Messenger. Each row shows the installed version, the latest available version, and a link to the manufacturer's page. At the bottom of the window, there is a note: 'Aceasta este o lista a aplicatiilor verificate de BitDefender si a actualizarilor disponibile (in cazul in care exista)'. The BitDefender logo is on the left, and 'Inainte' and 'Anuleaza' buttons are on the right.

Nume aplicatie	Versiune instalata	Ultima versiune	Stare
Yahoo! Messenger	9.0.0.2152	9.0.0.2162	Vizualizare pagina producator
Firefox	2.0.0.20 (en-US)	3.5.2	Vizualizare pagina producator
Windows Live Messenger	4,7,0,3000	14.0.8064.0206	Vizualizare pagina producator

Aceasta este o lista a aplicatiilor verificate de BitDefender si a actualizarilor disponibile (in cazul in care exista).

Aplicații

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

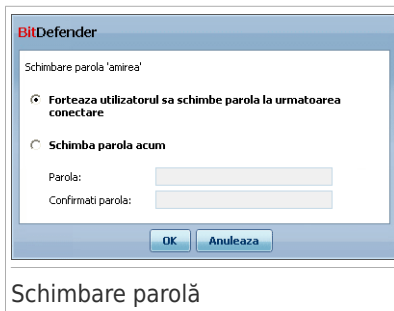
Faceți clic pe **Înainte**.

11.3.5. Pasul 5/6 - Schimbați parolele simple



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

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



Selectați metoda de rezolvare a acestei probleme:

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



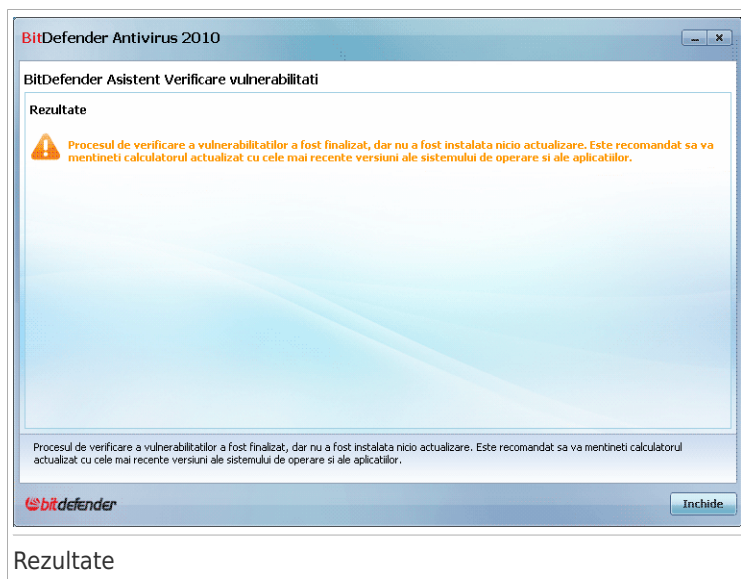
Notă

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

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

Faceți clic pe **Înainte**.

11.3.6. Pasul 6/6 - Examinați rezultatele



Faceți clic pe **Închide**.

Modul Intermediar

12. Pagina de stare

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



Pagina de stare

Pagina de stare conține următoarele secțiuni:

- **Stare generală** - Arată câte probleme afectează securitatea calculatorului dumneavoastră și vă ajută să le rezolvați. Dacă există probleme în așteptare, veți vedea un **cerc roșu cu semnul exclamării** și butonul **Remediază**. Faceți clic pe buton pentru a porni asistentul **Remediază probleme**.
- **Detalii stare** - Indică starea fiecărui modul principal folosind propoziții explicite și una dintre următoarele iconițe:
 - ✓ **Cerc verde cu bifă:** Nicio problemă de securitate. Calculatorul și datele dvs sunt protejate.
 - ✗ **Cerc gri cu semnul exclamării:** Activitatea componentelor acestui modul nu este monitorizată. Prin urmare, nu sunt disponibile informații legate de starea lor de securitate. Pot exista anumite probleme legate de acest modul.
 - ! **Cerc roșu cu semnul exclamării:** Mai multe probleme afectează securitatea sistemului dumneavoastră. Problemele majore necesită atenția dvs imediat. Problemele minore trebuie remediate cât mai curând.

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

● **Profil utilizator** - Indică profilul de utilizator selectat în acel moment și oferă un link către o sarcină relevantă pentru acesta:

- ▶ La selectarea profilului **Tipic**, butonul **Scanează acum** vă permite să efectuați o Scanare de sistem folosind **Asistentul de Scanare antivirus**. Va fi scanat întregul sistem, cu excepția arhivelor. În configurația implicită, se scanează după toate tipurile de aplicații periculoase, altele decât cele de tip **rootkit**.
- ▶ La selectarea profilului **Jucător**, butonul **Pornește/oprește Modul pentru jocuri** vă permite să activați/dezactivați **Modul pentru jocuri**. Modul pentru jocuri modifică temporar setările produsului pentru a minimiza impactul acestora asupra performanței sistemului.
- ▶ La selectarea profilului **Personal**, butonul **Actualizează acum** pornește imediat actualizarea. Va apărea o nouă fereastră în care puteți vedea starea actualizării.

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

13. Antivirus

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



Antivirus

Modulul Antivirus conține două secțiuni:

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

13.1. Zona de stare

În zona de stare puteți vedea lista completă a componentelor modulelor de securitate și starea lor curentă. Ca urmare a monitorizării fiecărui modul de securitate, BitDefender vă va avertiza când configurați setări care ar putea afecta securitatea calculatorului dvs, dar și atunci când ați uitat să efectuați sarcini importante.

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

- ✓ **Cerc verde cu bifă:** Nicio problemă nu afectează componenta.

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

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

13.1.1. Configurarea monitorizării stării

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



Important

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

Starea următoarelor componente de securitate poate fi monitorizată de BitDefender:

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


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

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

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

13.2. Sarcini rapide

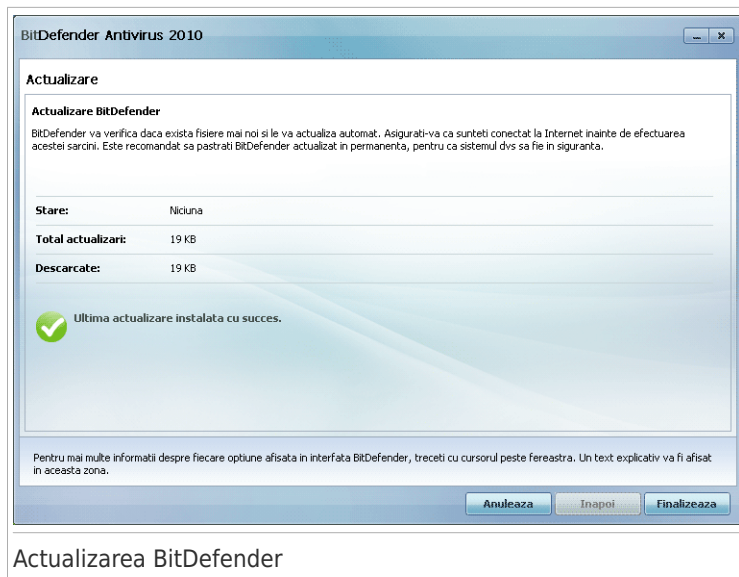
Aici găsiți linkuri către cele mai importante sarcini de securitate:

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

13.2.1. Actualizarea BitDefender

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

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



Actualizarea BitDefender

În această fereastră puteți vedea stadiul procesului de actualizare.

Procesul de actualizare este realizat progresiv, ceea ce înseamnă că fișierele care trebuie actualizate sunt înlocuite unul câte unul. Astfel, procesul de actualizare nu va afecta funcționarea produsului și, în același timp, orice vulnerabilitate va fi exclusă.

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



Notă

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

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

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

13.2.2. Scanarea cu BitDefender

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

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



Notă

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

Când rulați o sarcină de Scanare de sistem, Scanare profundă de sistem sau Scanare Documentele mele, va apărea un asistent de Scanare Antivirus. Urmați programul asistent în trei pași pentru a realiza procesul de scanare. Pentru informații detaliate despre acest program asistent, consultați secțiunea „*Programul asistent de scanare*” (p. 54).

Când rulați o Scanare personalizată, Asistentul de Scanare personalizată vă va ghida de-a lungul procesului. Urmați procedura în șase pași pentru a scana anumite fișiere sau directoare. Pentru informații detaliate despre acest program asistent, consultați secțiunea „*Asistent scanare personalizată*” (p. 58).

14. Antiphishing

BitDefender include un modul Antiphishing care verifică dacă paginile web pe care le accesați prin intermediul Internet Explorer sau Firefox sunt sigure. Pentru a accesa modulul Antiphishing, faceți clic pe tabul **Antiphishing**.



Modulul Antiphishing conține două secțiuni:

- **Zonă stare** - Afișează starea curentă a modulului antiphishing și vă permite să activați/dezactivați monitorizarea activității acestuia.
- **Sarcini rapide** - Aici puteți găsi linkuri către sarcini de securitate importante: actualizare imediată, scanare de sistem și scanare profundă de sistem.

14.1. Zona de stare

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

- ✓ **Cerc verde cu bifă:** Nicio problemă nu afectează componenta.
- ! **Cerc roșu cu semnul exclamării:** Mai multe probleme afectează componenta.

Descrierile problemelor apar în roșu. Faceți clic pe butonul **Remediază** din dreptul unei descrieri pentru a remedia problema semnalată.

Problema cea mai frecvent raportată pentru acest modul este **Antiphishing dezactivat**. Aceasta înseamnă că protecția Antiphishing nu este activată pentru niciuna dintre sau pentru unele dintre următoarele aplicații admise: Internet Explorer, Mozilla Firefox, Yahoo! Messenger sau Windows Live Messenger.

14.2. Sarcini rapide

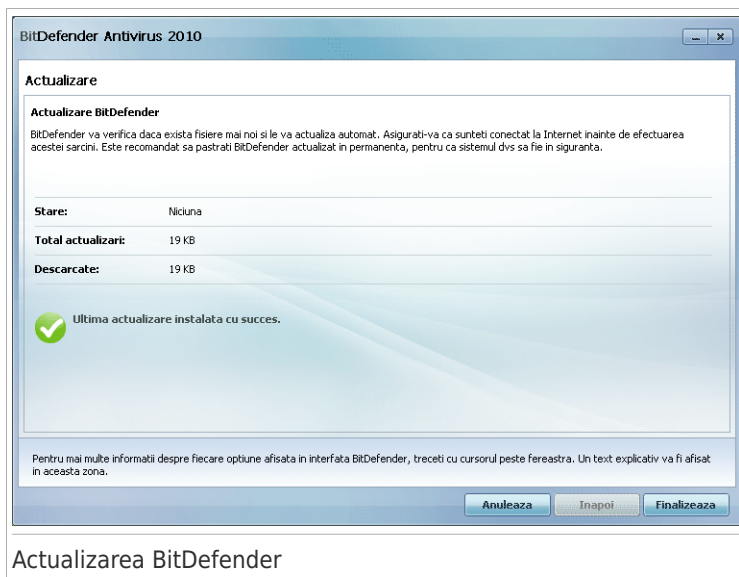
Aici găsiți linkuri către cele mai importante sarcini de securitate:

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

14.2.1. Actualizarea BitDefender

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

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



În această fereastră puteți vedea stadiul procesului de actualizare.

Procesul de actualizare este realizat progresiv, ceea ce înseamnă că fișierele care trebuie actualizate sunt înlocuite unul câte unul. Astfel, procesul de actualizare nu va afecta funcționarea produsului și, în același timp, orice vulnerabilitate va fi exclusă.

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



Notă

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

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

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

14.2.2. Scanarea cu BitDefender

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

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



Notă

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

Când rulați o sarcină de Scanare de sistem sau de Scanare profundă de sistem, va apărea asistentul de Scanare Antivirus. Urmați programul asistent în trei pași pentru

a realiza procesul de scanare. Pentru informații detaliate despre acest program asistent, consultați secțiunea „*Programul asistent de scanare*” (p. 54).

15. Vulnerabilitate

BitDefender include un modul Vulnerabilitate care vă ajută să mențineți actualizate aplicații critice de pe calculatorul dumneavoastră. Pentru a monitoriza și remedia vulnerabilitățile sistemului dumneavoastră, faceți clic pe tabul **Vulnerabilitate**.



Modulul Vulnerabilitate conține două secțiuni:

- **Zonă stare** - Afișează starea curentă a modului Verificare vulnerabilități și vă permite să activați/dezactivați monitorizarea activității acestuia.
- **Sarcini rapide** - Aici puteți găsi un link către Asistentul Verificare vulnerabilități.

15.1. Zona de stare

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

- ✓ **Cerc verde cu bifă:** Nicio problemă nu afectează componenta.
- ⚠ **Cerc roșu cu semnul exclamării:** Mai multe probleme afectează componenta.

Descrierile problemelor apar în roșu. Faceți clic pe butonul **Remediază** sau **Instalează** din dreptul unei descrieri, pentru a remedia problema semnalată.

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

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

15.2. Sarcini rapide

O singură sarcină este disponibilă:

- **Scanare vulnerabilități** - pornește programul asistent care verifică sistemul de vulnerabilități și vă ajută să le rezolvați.

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

Pentru a verifica dacă există puncte vulnerabile ale calculatorului dvs, faceți clic pe **Scanare vulnerabilități** și urmați pașii „*Asistent Verificare vulnerabilități*” (p. 66)

16. Rețea

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



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

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

16.1. Sarcini rapide

Inițial, un singur buton este disponibil.

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

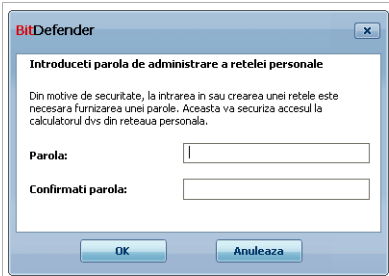
După intrarea în rețea, vor apărea mai multe butoane.

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

16.1.1. Intrarea în rețeaua BitDefender

Pentru a fi în rețeaua BitDefender personală, urmați acești pași:

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



The screenshot shows a dialog box titled "BitDefender" with a close button (X) in the top right corner. The main text reads: "Introduceți parola de administrare a rețelei personale" (Enter the network administration password). Below this, a smaller text block explains: "Din motive de securitate, la intrarea în sau crearea unei rețele este necesară furnizarea unei parole. Aceasta va securiza accesul la calculatorul dvs din rețeaua personală." (For security reasons, when entering or creating a network, it is necessary to provide a password. This will secure access to your computer from the personal network.) There are two input fields: "Parola:" (Password) and "Confirmați parola:" (Confirm password). At the bottom, there are two buttons: "OK" and "Anulează" (Cancel). Below the dialog box, the text "Configurare parolă" (Password configuration) is visible.

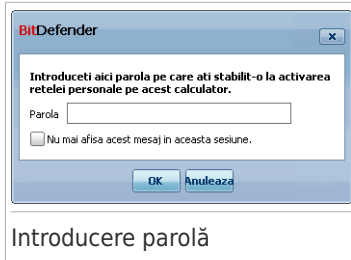
2. Introduceți aceeași parolă în ambele câmpuri editabile.
 3. Faceți clic pe **OK**.
- Puteți vedea numele calculatorului apărând pe harta rețelei.

16.1.2. Adăugarea calculatoarelor la rețeaua BitDefender

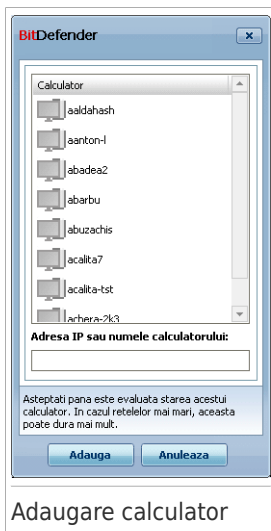
Înainte de a putea adăuga un calculator la rețeaua BitDefender personală, trebuie să configurați parola rețelei BitDefender pe calculatorul respectiv.

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




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



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



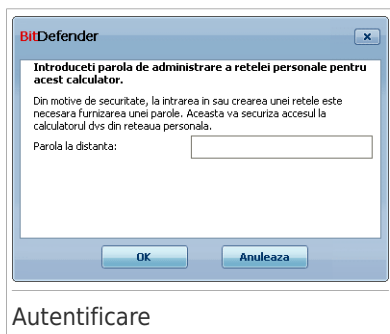
Puteți vedea lista calculatoarelor din rețea. Sensul iconițelor este după cum urmează:

-  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.



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

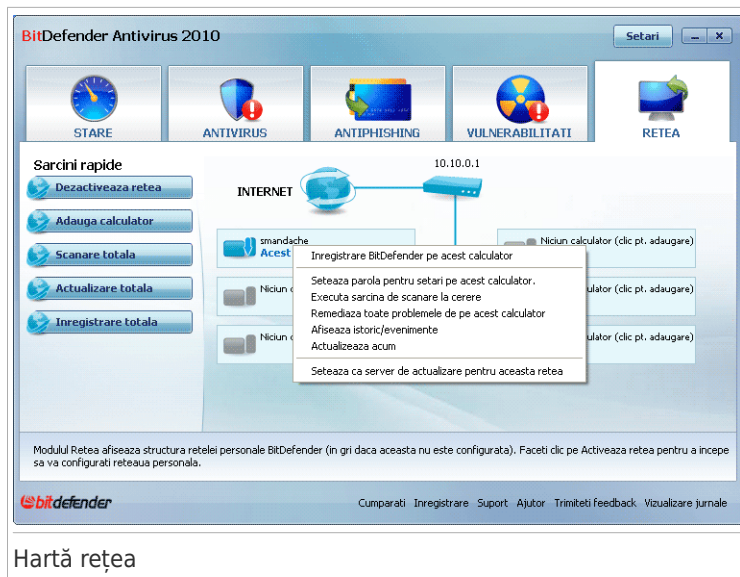


Notă

Puteți adăuga până la cinci calculatoare pe harta rețelei.

16.1.3. Administrarea rețelei BitDefender

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



Hartă rețea

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

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

● Scoate calculatorul din rețeaua personală

Vă permite să scoateți un calculator din rețea.

● Înregistrează BitDefender pe acest calculator

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

● Stabilește o parolă pentru setări pe un calculator la distanță

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

● Execută o sarcină de scanare la cerere

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

● Remediază toate problemele de pe acest calculator

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

● Vizualizare istoric/evenimente

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

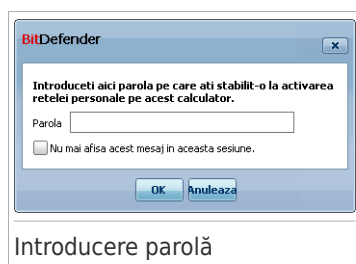
● Update Now

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

● Stabilește acest calculator ca server de actualizare al acestei rețele

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

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



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



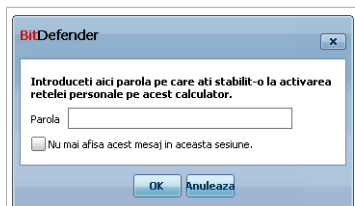
Notă

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

16.1.4. Scanarea tuturor calculatoarelor

Pentru a scana toate calculatoarele administrate, urmați acești pași:

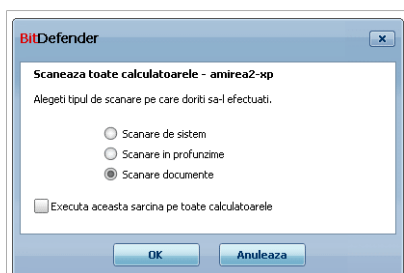
1. Faceți clic pe **Scanează tot**. Vi se va cere să furnizați parola locală de administrare a rețelei.



Introducere parolă

2. Selectați tipul de analiză.

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



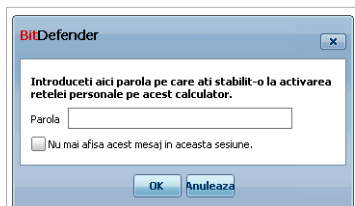
Selectați tipul de analiză.

3. Faceți clic pe **OK**.

16.1.5. Actualizarea tuturor calculatoarelor

Pentru a actualiza toate calculatoarele administrate, urmați acești pași:

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



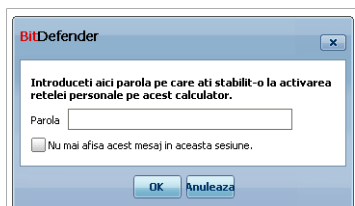
Introducere parolă

2. Faceți clic pe **OK**.

16.1.6. Înregistrarea tuturor calculatoarelor

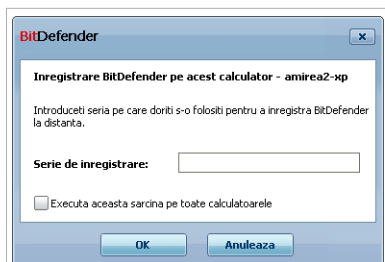
Pentru a înregistra toate calculatoarele administrate, urmați acești pași:

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



Introducere parolă

2. Introduceți cheia cu care doriți să înregistrați produsele.



Înregistrează tot

3. Faceți clic pe **OK**.

Modul Expert

17. General

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

17.1. Pagina de stare

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

BitDefender Antivirus 2010

Stare Setari Info sistem

General

- Antivirus
- Control date
- Vulnerabilitati
- Criptare
- Mod jocuri/laptop
- Retea personala
- Actualizare
- Inregistrare

Stare securitate

AVERTISMENT: 9 probleme de securitate afecteaza acest calculator. Remediaza

Configurare monitorizare stare

Statistici		Descriere generala	
Fisiere scanate:	1183	Ultima actualizare:	niciodata
Fisiere dezinfectate:	0	BitDefender Cont:	testare.automata@mall...
Fisiere infectate detectate:	0	Inregistrare:	Valid
Ultima scanare:	niciodata	Expira in:	<div style="width: 100%; height: 10px; background-color: green;"></div>
Urmatoarea scanare:	8/25/2009 2:00:00 AM		322 zile

Activitate fisiere

Modulul Stare afiseaza starea de securitate a produsului dvs si linkuri catre cele mai importante module ale produsului dvs.

Reinnoire Inregistrare Suport Ajutor Trimiteti feedback Vizualizare jurnale

Pagina de stare

Pagina de stare conține mai multe secțiuni:

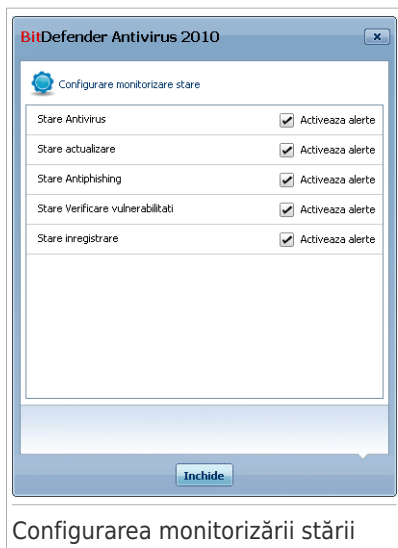
- **Stare generală** - Vă informează despre orice probleme care afectează securitatea calculatorului dvs.
- **Statistici** - Afixează informații importante referitoare la activitatea BitDefender.
- **Prezentare generală** - Afixează informații referitoare la actualizare, contul dumneavoastră, înregistrare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

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

17.1.1. Stare Generală

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

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



Configurarea monitorizării stării

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

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

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

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

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

- **Antiphishing** - BitDefender monitorizează starea modului Antiphishing. Dacă nu este activat pentru toate aplicațiile admise, se va raporta problema **Antiphishing dezactivat**.
- **Verificare vulnerabilități** - BitDefender monitorizează caracteristica verificare vulnerabilități. Aceasta vă permite să aflați dacă e necesar să instalați actualizări Windows, ale aplicațiilor sau dacă e nevoie să modificați o parolă vulnerabilă.
Cele mai frecvente probleme raportate pentru această componentă sunt prezentate în tabelul de mai jos.

Stare	Descriere
Verificare vulnerabilități dezactivată	BitDefender nu verifică dacă există vulnerabilități legate de actualizări Windows lipsă, aplicarea actualizărilor sau stabilirea unor parole simple.

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



Important

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

17.1.2. Statistici

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

Element	Descriere
Fișiere scanate	Indică numărul de fișiere care au fost verificate după malware la ultima scanare.
Fișiere dezinfectate	Indică numărul de fișiere care au fost dezinfectate la ultima scanare.
Fișiere infectate detectate	Indică numărul de fișiere infectate detectate în sistemul dumneavoastră la ultima scanare.
Ultima scanare de sistem	Aată când a fost scanat ultima oară calculatorul dumneavoastră. Dacă ultima scanare a fost efectuată cu mai mult de o săptămână în urmă, scanați calculatorul cât mai repede posibil. Pentru a scana tot calculatorul, mergeți la Antivirus , tabul Scanare viruși și rulați una dintre aceste sarcini: Scanare profundă sistem sau Scanare completă sistem.

Element	Descriere
Următoarea scanare	Arată când urmează să fie scanat calculatorul dumneavoastră.

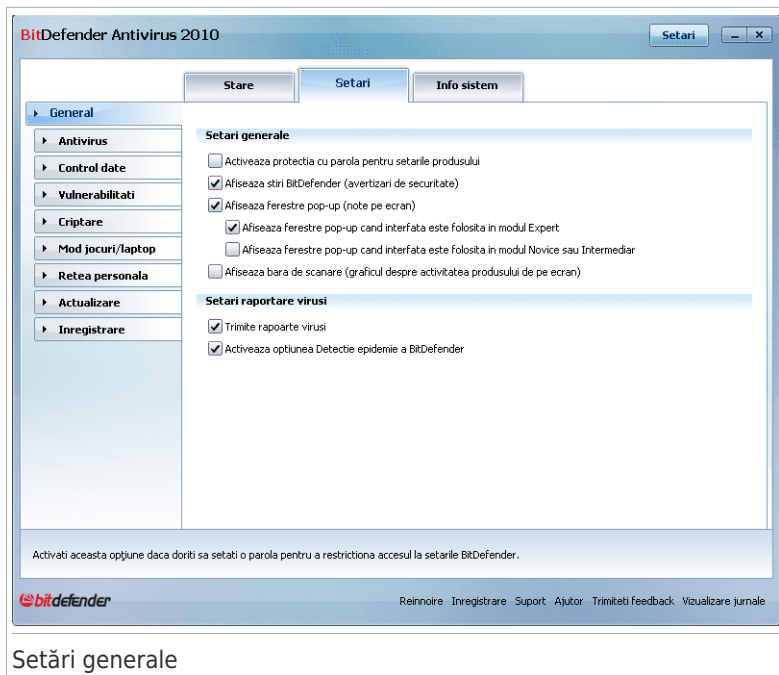
17.1.3. Descriere generală

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

Element	Descriere
Ultima actualizare	Arată când a fost actualizat ultima oară produsul dumneavoastră BitDefender. Vă rugăm să efectuați actualizări în mod regulat, pentru a avea un sistem complet protejat.
Cont BitDefender	Indică adresa de e-mail pe care o puteți utiliza pentru a vă accesa contul online, unde vă puteți recupera seria de înregistrare pierdută și puteți beneficia de suport BitDefender și alte servicii personalizate. Trebuie să creați un cont BitDefender pentru a activa produsul. Pentru a afla informații despre contul BitDefender, consultați secțiunea „ <i>Înregistrare și Contul meu</i> ” (p. 49).
Înregistrare	Indică tipul și starea seriei dumneavoastră de înregistrare. Pentru a menține securitatea sistemului dumneavoastră, trebuie să reînnoiți sau să actualizați versiunea BitDefender în cazul în care seria dumneavoastră a expirat.
Expiră în	Indică numărul de zile rămase până la expirarea seriei de înregistrare. Dacă seria dumneavoastră de înregistrare expiră în următoarele zile, vă rugăm să înregistrați produsul cu o nouă serie de înregistrare. Pentru a achiziționa o serie de înregistrare sau pentru a vă reînnoi licența, faceți clic pe linkul Cumpără , situat în partea de jos a ferestrei.

17.2. Setări

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



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

17.2.1. Setări generale

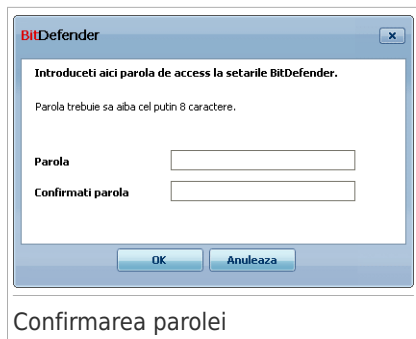
- **Activează protecția prin parolă pentru setările produsului** - permite setarea unei parole pentru a proteja configurația BitDefender.



Notă

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

Dacă selectați această opțiune, va apărea următoarea fereastră:



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

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



Important

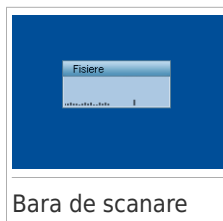
Dacă uitați parola va fi nevoie să reparați produsul pentru a schimba configurarea BitDefender.

- **Afișează știri BitDefender (avertizări de securitate)** - afișează din când în când notificări de securitate referitoare la noi viruși descoperiți, trimise de serverul BitDefender.
- **Afișează ferestre pop-up (note pe ecran)** - afișează ferestre de informare cu privire la starea produsului. Puteți configura BitDefender să afișeze ferestre pop-up numai atunci când interfața este în Modul Novice/Intermediar sau Expert.
- **Afișează bara de scanare (graficul de pe ecran al activității produsului)** - afișează **Bara de scanare** atunci când vă conectați la Windows. Debifați această căsuță dacă nu doriți ca bara de scanare să mai fie afișată.



Notă

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



17.2.2. Setări raportare viruși

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

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

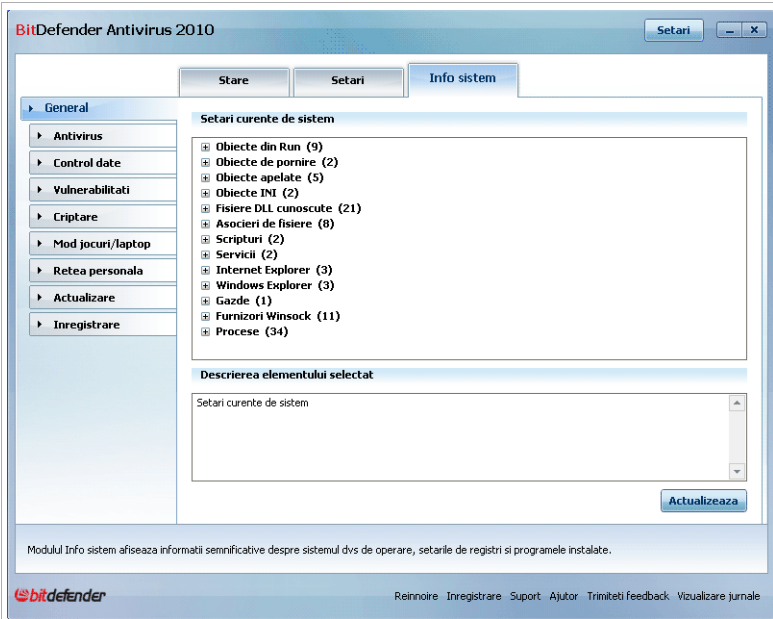
- **Activează Detecția epidemiilor virale de către BitDefender** - trimite Laboratorului BitDefender rapoarte referitoare la potențiale epidemii virale.

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

17.3. Informații sistem

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

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



The screenshot shows the BitDefender Antivirus 2010 interface. The window title is "BitDefender Antivirus 2010" with a "Setari" button and window controls. The main area has three tabs: "Stare", "Setari", and "Info sistem". The "Info sistem" tab is active, showing a left sidebar with a tree view under "General" containing: "Antivirus", "Control date", "Vulnerabilitati", "Criptare", "Mod jocuri/laptop", "Retea personala", "Actualizare", and "Inregistrare". The main content area is titled "Setari curente de sistem" and contains a list of system objects with expandable icons and counts: "Obiecte din Run (9)", "Obiecte de pornire (2)", "Obiecte apelate (5)", "Obiecte INI (2)", "Fisiere DLL cunoscute (21)", "Asocieri de fisiere (8)", "Scripturi (2)", "Servicii (2)", "Internet Explorer (3)", "Windows Explorer (3)", "Gazde (1)", "Furnizori Winsock (11)", and "Procese (34)". Below this list is a section "Descrierea elementului selectat" with a text area containing "Setari curente de sistem" and an "Actualizeaza" button. At the bottom, there is a footer with the BitDefender logo and links: "Reinnoire Inregistrare Suport Ajutor Trimiteți feedback Vizualizare jurnale".

Informații sistem

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

Sunt disponibile trei butoane:

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



Notă

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

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

18. Antivirus

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

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



Notă

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

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

18.1. Protecție în timp real

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

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

BitDefender Antivirus 2010 [Setari] [X]

Scut | Scanare virusi | Excluderi | Quarantine

General | Antivirus | Control date | Vulnerabilitati | Criptare | Mod jocuri/laptop | Retea personala | Actualizare | Inregistrare

Protectia in timp real este activata
 Ultima scanare: niciodata
[Scaneaza acum](#)

Nivel protectie

Agresiv **IMPLICIT - Securitate standard, consum scazut de resurse**
 - Scaneaza toate fisierele
 - Scaneaza mesajele e-mail primite si trimise
 - Scaneaza dupa virusi si programe spion
 - Nu scaneaza traficul web (HTTP)
 Implicit
 - Actiuni pentru fisierele infectate: Dezinfecteaza fisierul, Muta fisierul in carantina
 - Scaneaza folosind B-HAVE (analiza euristica)
 - Scaneaza traficul de mesaje instant
 Permisiv

[Nivel personal] [Nivel implicit] [Setari avansate]

Antiphishing activat
 Activeaza Antiphishing pentru Microsoft Windows Internet Explorer
 Activeaza Antiphishing pentru Mozilla Firefox
 Activeaza Antiphishing pentru Yahoo Messenger
 Activeaza Antiphishing pentru Microsoft Windows Live Messenger
[Lista alba](#)

Penru mai multe informatii despre fiecare optiune afisata in interfața BitDefender, treceti cu cursorul peste fereastra. Un text explicativ va fi afisat in aceasta zona.

bitdefender Reinnoire Inregistrare Suport Ajutor Trimiteti feedback Vizualizare jurnale

Protectie 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 virusi, păstrați **Protectia in timp real** activată.

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

18.1.1. Configurarea nivelului de protecție

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

Există trei nivele de protecție:

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

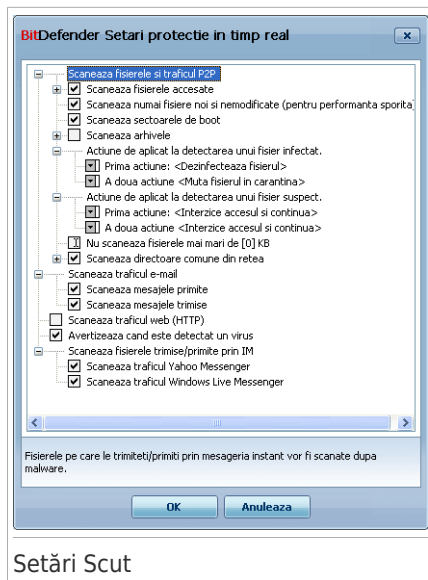
Nivel de protecție	Descriere
	Numai aplicațiile și mesajele e-mail primite sunt scanate împotriva virușilor. Pe lângă metoda clasică de scanare bazată pe semnături, se utilizează și analiza euristică. Acțiunile aplicate fișierelor infectate sunt următoarele: dezinfectare/mutare în carantină.
Standard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

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

18.1.2. Personalizarea nivelului de protecție

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

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



Setări Scut

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



Notă

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

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

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

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

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

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

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

Următoarele opțiuni sunt disponibile:

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

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

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

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

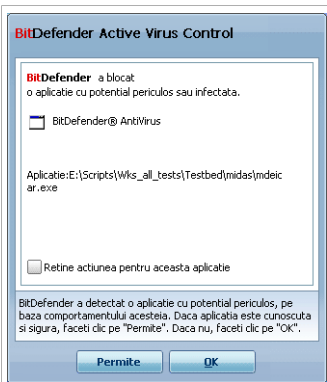
- **Scanează fișierele primite/trimise prin IM.** Pentru a scana fișierele trimise sau primite prin intermediul Yahoo Messenger sau Windows Live Messenger, selectați căsuțele corespunzătoare.

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

18.1.3. Configurarea setărilor Active Virus Control

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

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



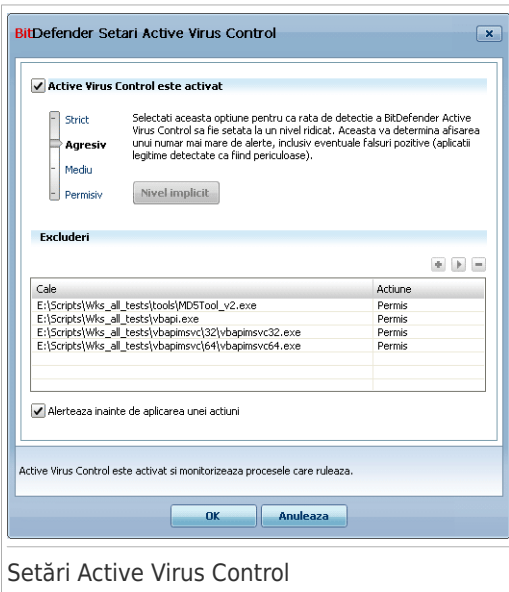
Alerta Active Virus Control

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

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

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

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



Setări Active Virus Control

Selecționați căsuța corespunzătoare pentru a activa Active Virus Control.



Important

Mențineți Active Virus Control activat pentru protecție împotriva virușilor necunoscuți.

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

Configurarea nivelului de protecție

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



Notă

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

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

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

Administrarea aplicațiilor sigure/nesigure

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

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

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

Pentru administrarea listei, folosiți butoanele de deasupra tabelului:

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

18.1.4. Dezactivarea protecției în timp real

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



Avertisment

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

18.1.5. Configurarea protecției antiphishing

BitDefender furnizează protecție antiphishing în timp real pentru:

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

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

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



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

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



Notă

Puteți adăuga ușor site-uri web pe lista albă din bara de comenzi BitDefender Antiphishing integrată în browserul dumneavoastră. Pentru mai multe informații, consultați „*Integrarea cu browserele web*” (p. 203).

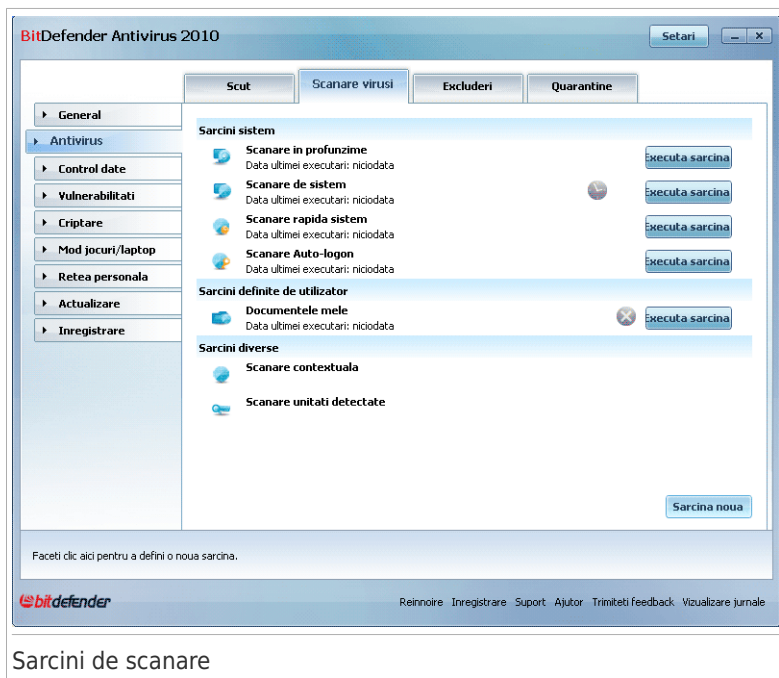
Pentru a șterge un site din lista albă, faceți clic pe butonul **Șterge** corespunzător. Faceți clic pe **Save** pentru a salva modificările și închide fereastra.

18.2. Scanarea la cerere

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

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

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



Sarcini de scanare

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

18.2.1. Sarcini de scanare

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

Există trei categorii de sarcini de scanare:

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

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



Notă

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

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

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

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

Fiecare sarcină are o fereastră de **Proprietăți** în care o puteți configura și puteți vedea jurnalele de scanare. Pentru a deschide această fereastră, faceți dublu-clic pe sarcină sau faceți clic pe butonul **Proprietăți** din fața numelui fiecărei sarcini. Pentru mai multe informații, consultați secțiunea „*Configurarea sarcinilor de scanare*” (p. 119).

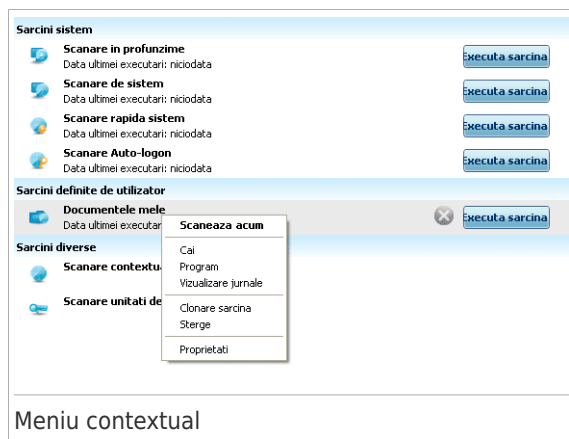
Pentru a rula o sarcină de scanare a sistemului sau definită de utilizator, faceți clic pe butonul **Rulează sarcina** corespunzător. Va apărea **programul asistent de scanare** care vă va ghida de-a lungul procesului de scanare.

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

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

18.2.2. Utilizarea meniului contextual

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



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

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



Notă

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

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



Notă

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

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

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

18.2.3. Crearea sarcinilor de scanare

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

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

18.2.4. Configurarea sarcinilor de scanare

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



Notă

Pentru mai multe informații despre vizualizarea rapoartelor și tabul **Rapoarte**, consultați *„Examinarea rapoartelor de scanare”* (p. 139).

Configurarea setărilor de scanare

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



Descriere generală

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

Alegerea nivelului de scanare

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

Există trei nivele de scanare:

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

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

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

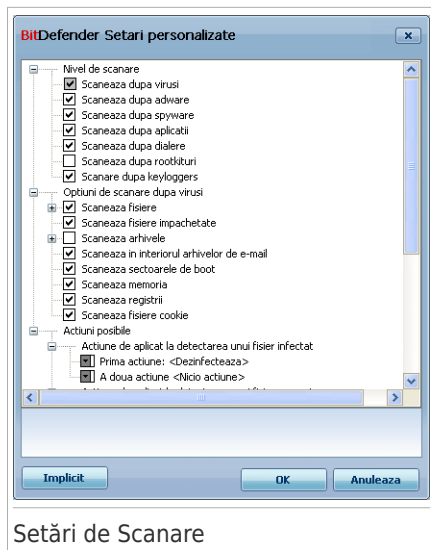
- **Executa procesul cu prioritate scăzută.** Reduce prioritatea procesului de scanare. Veți permite altor programe să ruleze cu o viteză superioară, dar timpul necesar pentru finalizarea scanării va crește.
- **Minimizează asistentul de scanare la bara de sistem.** Minimizează fereastra de scanare **bara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

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

Personalizarea nivelului de scanare

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

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



Setări de Scanare

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

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

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

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

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

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



Notă

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

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

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

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

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



Notă

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

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

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



Notă

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

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

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

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

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

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

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

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

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

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

Setarea locației de scanare

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



Locație scanare

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

Următoarele butoane sunt disponibile:

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



Notă

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

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



Notă

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

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

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



Notă

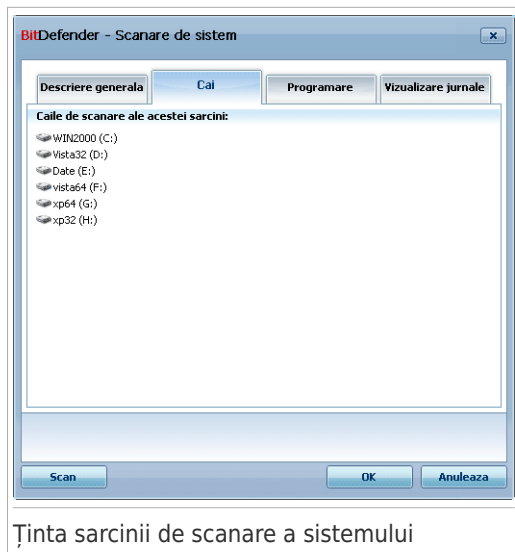
Dacă doriți să vă scanați tot sistemul, selectați opțiunea **Toate obiectele**.

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

Verificarea căii de scanare a sarcinilor de sistem

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

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



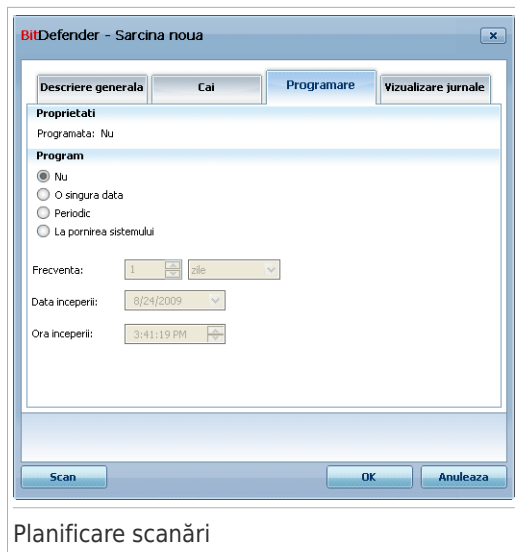
Sarcinile **Scanare de sistem** și **Scanare profundă de sistem** scanează toate partițiile locale, în timp ce sarcina **Scanare rapidă de sistem** scanează doar directoarele Windows și Program Files.

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

Planificarea sarcinilor de scanare

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

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



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

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

- **Nu** - lansează sarcina numai la cererea utilizatorului.
- **O singură dată** - sarcina este executată o singură dată, la un anumit moment. Specificați data și timpul lansării în execuție în câmpurile **Data începerii/Ora începerii**.
- **Periodic** - lansează scanarea periodic, la anumite intervale de timp (minute, ore, zile, săptămâni, luni), începând de la o dată și o oră precizate.
Dacă doriți ca scanarea să se repete la anumite intervale de timp, selectați opțiunea **Periodic** și introduceți în câmpul de editare **La fiecare** numărul de minute/ore/zile/săptămâni /luni reprezentând frecvența acestui proces. De asemenea, trebuie să specificați data și ora lansării în execuție în câmpurile **Datai/Ora începerii**.
- **La pornirea sistemului** - sarcina este executată la numărul de minute specificat după ce un utilizator s-a conectat la Windows.

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

18.2.5. Scanarea fișierelor și directorelor

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



Notă

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

Sugestii pentru scanare

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

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

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

- Dacă descărcați în mod frecvent fișiere de pe Internet într-un anumit director, creați o sarcină nouă de scanare și **setați directorul respectiv ca locație de scanare**. Programați sarcina să ruleze în fiecare zi sau mai des.
- Un anumit tip de aplicații malițioase modifică setările Windows pentru a fi lansate automat la pornirea sistemului. Pentru a vă proteja calculatorul împotriva unor astfel de aplicații periculoase, puteți programa sarcina **Scanare automată la conectare** să ruleze automat la pornirea sistemului. Vă rugăm să țineți cont că scanarea autologon poate afecta funcționarea sistemului pentru o scurtă perioadă de timp după pornire.

Metode de scanare

BitDefender oferă patru tipuri de scanare la cerere:

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

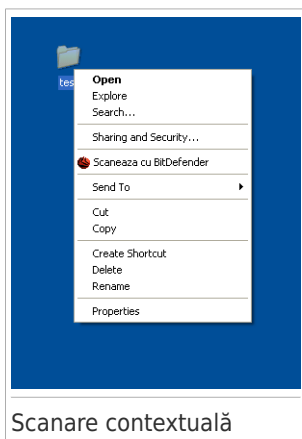
Scanare imediată

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

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

Scanare contextuală

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



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

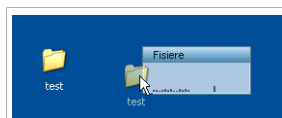
Puteți modifica opțiunile de scanare și examina fișierele de raport accesând fereastra de **Proprietăți** a sarcinii **Scanare meniu contextual**.

Scanare prin drag&drop

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



Trageți fișierul



Lăsați fișierul

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

Scanare manuală

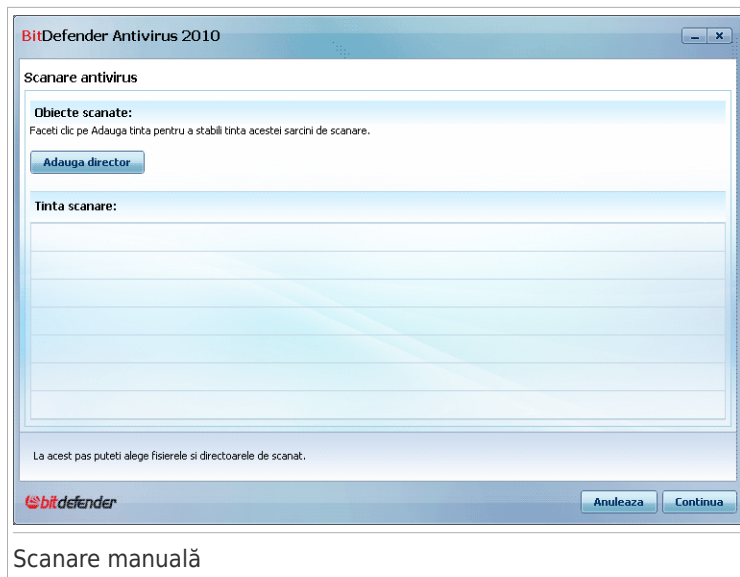
Scanarea manuală constă în selectarea directă a obiectului ce trebuie scanat utilizând opțiunea Scanare manuală BitDefender din grupul BitDefender din meniul Start.



Notă

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

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



Scanare manuală

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

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


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

Programul asistent de scanare

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

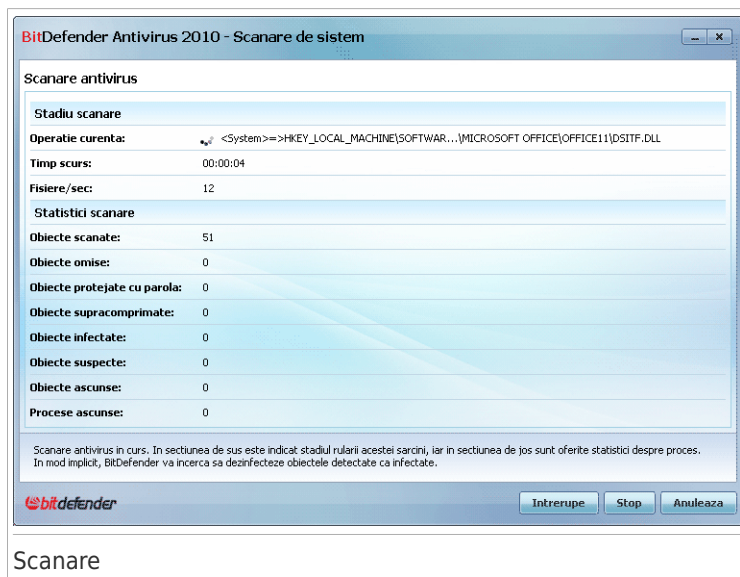


Notă

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

Pasul 1/3 - Scanare

BitDefender va începe scanarea obiectelor selectate.



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

Așteptați ca BitDefender să finalizeze scanarea.



Notă

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

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

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

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

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

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

Pasul 2/3 - Selectați acțiunile

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



Acțiuni

Puteți vedea numărul problemelor care vă afectează sistemul.

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

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

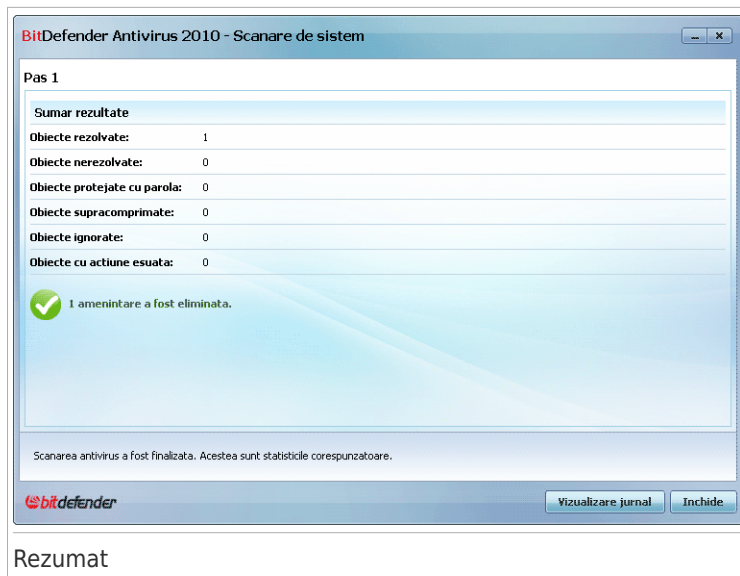
Una sau mai multe dintre opțiunile următoare pot apărea în meniu:

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

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

Pasul 3/3 - Examinați rezultatele

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



Rezumat

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



Important

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

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

BitDefender nu a putut remedia anumite probleme

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

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

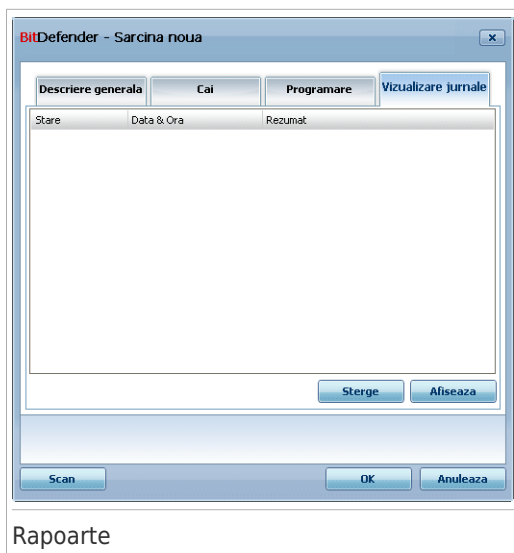
BitDefender a detectat fișiere suspecte

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

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

18.2.6. Examinarea rapoartelor de scanare

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



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

Sunt disponibile două butoane:

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



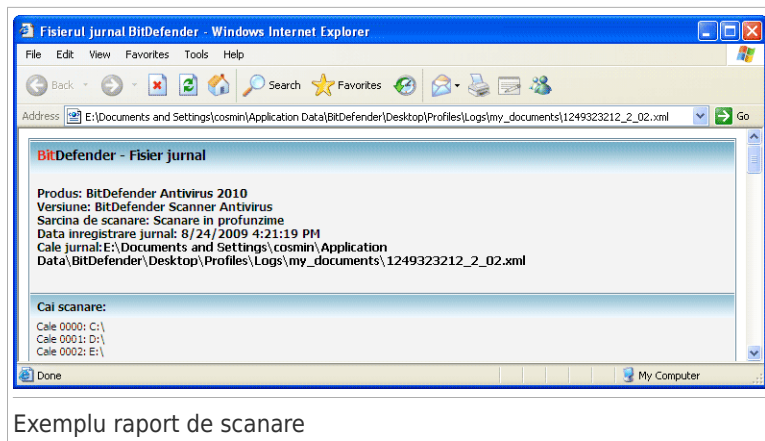
Notă

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

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

Exemplu raport de scanare

Imaginea următoare reprezintă un exemplu de raport de scanare:



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

18.3. Obiecte excluse de la scanare

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

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

Pot fi excluse de la scanare două tipuri de obiecte:

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




Notă

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

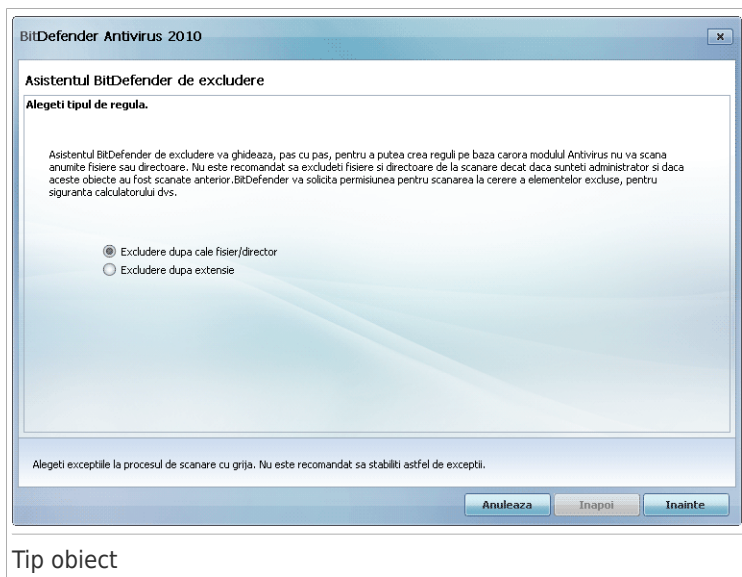
Pentru a vedea și administra obiectele excluse de la scanare, mergeți la **Antivirus>Excepții** în Modul Expert.

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**.

18.3.1. Excluderea căilor de la scanare

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

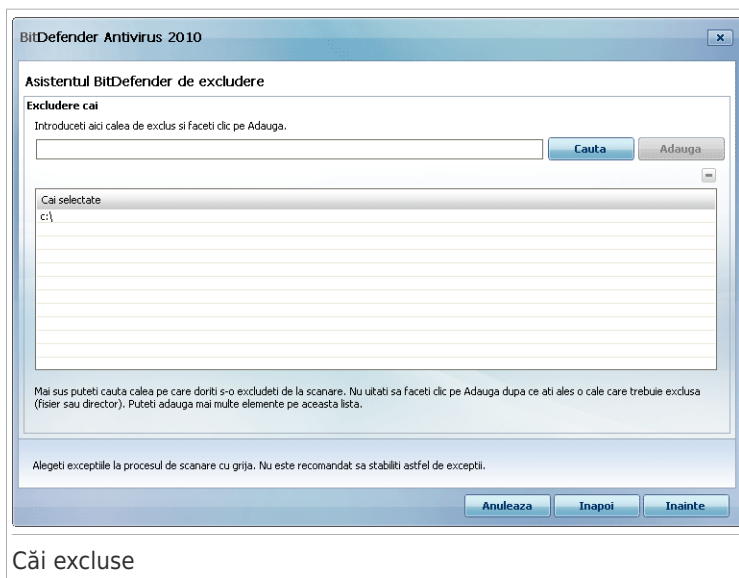
Pasul 1/4 - Selectați tipul obiectului



Selectați opțiunea de excludere a unei căi de la scanare.

Faceți clic pe **Înainte**.

Pasul 2/4 - Specificați căile excluse



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

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



Notă

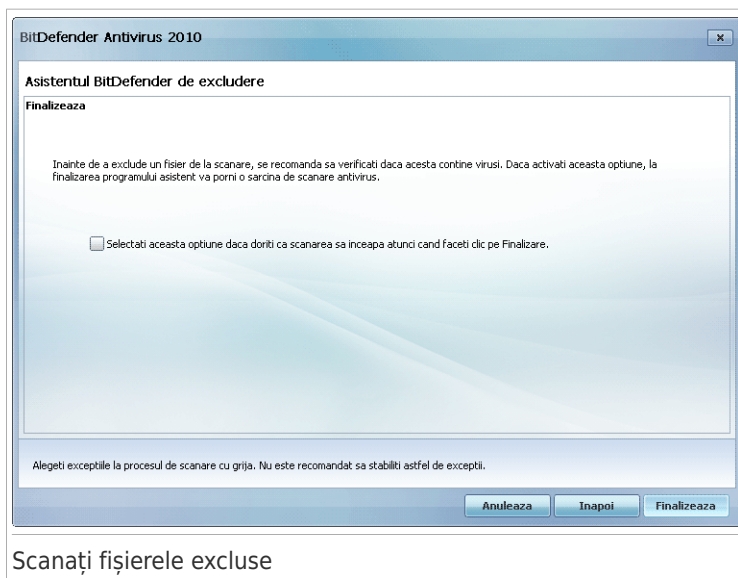
Un mesaj de eroare va apărea dacă nu există calea furnizată. Faceți clic pe **OK** și verificați validitatea căii.

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

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

Faceți clic pe **Înainte**.

Pasul 4/4 - Scanați fișierele excluse



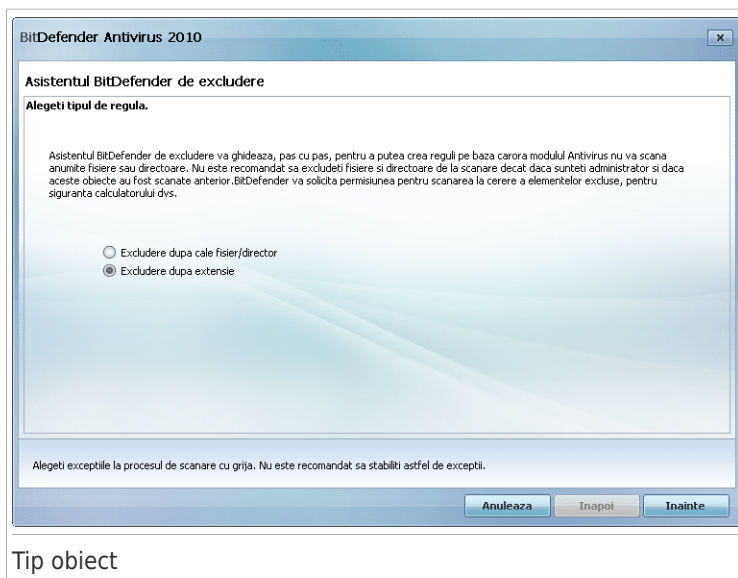
Este recomandat să scanați fișierele din locațiile specificate pentru a vă asigura că acestea nu sunt infectate. Selectați căsuța pentru a scana aceste fișiere înainte de a le exclude de la scanare.

Faceți clic pe **Finalizare**.

18.3.2. Excluderea extensiilor de la scanare

Pentru a exclude extensiile 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.

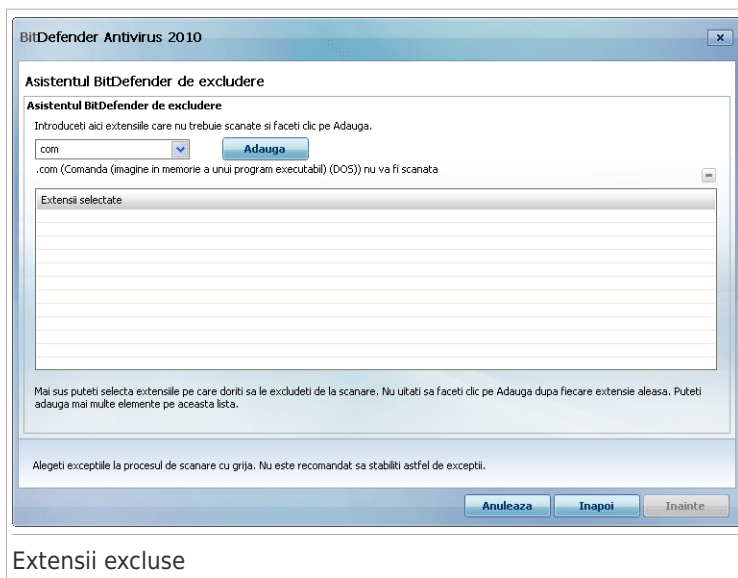
Pasul 1/4 - Selectați tipul obiectului



Selectați opțiunea de excludere a extensiilor de la scanare.

Faceți clic pe **Înainte**.

Pasul 2/4 - Specificați extensiile excluse



Extensii excluse

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

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



Notă

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

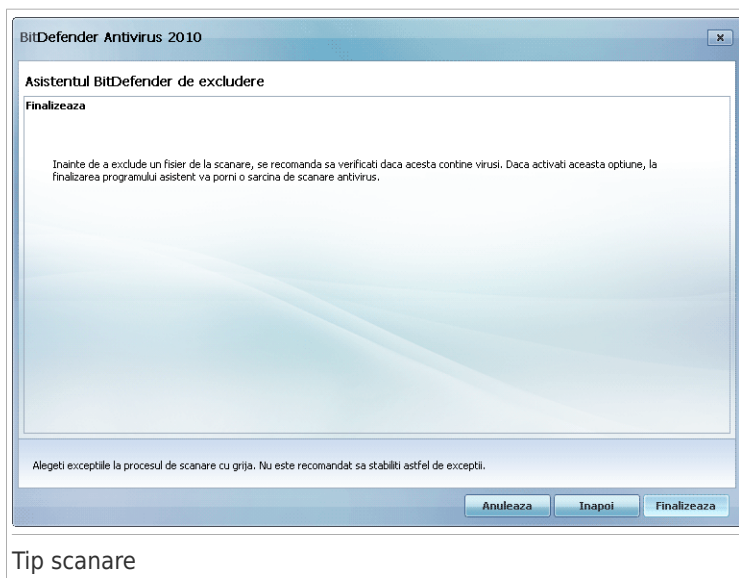
- Introduceți extensia care doriți să fie exclusă de la scanare și faceți clic pe **Adaugă**.

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

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

Faceți clic pe **Înainte**.

Pasul 4/4 - Selectați tipul de scanare



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

Faceți clic pe **Finalizare**.

18.4. Zona de carantină

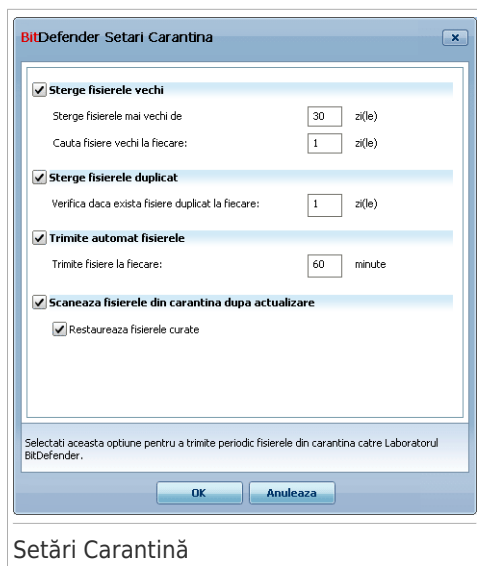
BitDefender permite izolarea fișierelor infectate sau suspecte într-o zonă sigură, numită carantină. Izolând aceste fișiere în carantină, riscul răspândirii infecției dispare, iar în plus, aveți posibilitatea să trimiteți aceste fișiere Laboratorului BitDefender pentru analiză aprofundată.

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

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

18.4.2. Configurarea setărilor carantinei

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



Setări Carantină

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

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



Notă

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

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



Notă

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

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



Notă

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

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

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

19. Control date

BitDefender monitorizează zeci de potențiale puncte sensibile ale sistemului dumneavoastră de operare, acolo unde pot acționa aplicațiile spyware, și verifică orice schimbare apărută. Acest modul blochează în mod eficient caii troieni și alte instrumente instalate de hackeri, care încearcă să vă dezvăluie identitatea și să trimită informațiile personale, cum ar fi seria cărții de credit, din computerul dumneavoastră, către hacker.

19.1. Status Control date

Pentru a configura Controlul datelor personale și a vedea informații legate de activitatea acestei opțiuni, faceți clic pe **Control date personale > Stare** în Modul Expert.

The screenshot shows the BitDefender Antivirus 2010 interface for the 'Control date personale' (Personal Data Control) settings. The window title is 'BitDefender Antivirus 2010' and it has a 'Setari' button in the top right corner. The left sidebar contains a tree view with categories: General, Antivirus, Control date (selected), Vulnerabilitati, Criptare, Mod jocuri/laptop, Retea personala, Actualizare, and Inregistrare. The main content area is divided into several sections:

- Stare:** A tabbed interface with 'Stare', 'Identitate', 'Registri', 'Cookie', and 'Script' tabs. The 'Stare' tab is active, showing a checked checkbox for 'Controlul datelor personale este activat' (Personal data control is activated) and a note: 'Controlul identității nu este configurat' (Identity control is not configured).
- Nivel protecție:** A vertical slider with three positions: 'Agresiv' (top), 'Implicit' (middle), and 'Permisiv' (bottom). To the right, under 'Personalizat', a list shows: '- Identitate Control activat', '- Registri Control activat', '- Cookie Control dezactivat', and '- Script Control dezactivat'. Below this list are two buttons: 'Nivel personal' and 'Nivel implicit'.
- Statistici Control date personale:** A table showing the following statistics:

Informații personale blocate:	0
Tentative acces la registri blocate:	0
Fisiere cookie blocate:	0
Scripturi blocate:	0

At the bottom of the window, there is a note: 'Modulul Control date personale este activat. Pentru siguranța datelor dvs, va recomandam sa mentineti acest modul activat permanent.' (The Personal Data Control module is activated. For your data security, we recommend you keep this module activated permanently.) The footer contains the BitDefender logo and links for 'Reinnoire', 'Inregistrare', 'Suport', 'Ajutor', 'Trimiteti feedback', and 'Vizualizare jurnale'.

Status Control date

Puteți vedea dacă este activat sau nu Controlul datelor. Pentru a schimba starea Controlului datelor, debifați sau selectați căsuța corespunzătoare.



Important

Pentru a preveni furtul de date și a vă proteja identitatea, mențineți activat **Controlul datelor**.

Controlul datelor vă protejează calculatorul prin intermediul următoarelor controale:

- **Controlul identității** - vă protejează datele confidențiale filtrând traficul web (HTTP), e-mail (SMTP) și de mesagerie instant la ieșirea din calculator potrivit regulilor create de dumneavoastră în secțiunea **Identitate**.
- **Controlul regiștrilor** - vă cere permisiunea de fiecare dată când un program încearcă să modifice informațiile din regiștri astfel încât să fie lansat la pornirea Windows.
- **Controlul fișierelor cookie** - vă cere permisiunea de fiecare dată când un site încearcă să seteze un cookie.
- **Controlul scripturilor** - vă cere permisiunea de fiecare dată când un domeniu încearcă să ruleze un script sau alt conținut activ.

În partea de jos a acestei secțiuni, puteți vedea **statisticile Controlului datelor**.

19.1.1. Configurarea nivelului de protecție

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

Există trei nivele de protecție:

Nivel de protecție	Descriere
Permisiv	Toate controalele de protecție sunt dezactivate.
Standard	Numai Control identitate este activat.
Agresiv	Control identitate , Control registri , Control fișiere cookie și Control script-uri sunt activate.

Puteți personaliza nivelul de protecție făcând clic pe **Nivel personal**. În fereastra care va apărea, selectați controalele de protecție pe care doriți să le activați și faceți clic pe **OK**.

Faceți clic pe **Nivel implicit** pentru a seta cursorul la nivelul implicit.

19.2. Control identitate

Păstrarea datelor confidențiale în siguranță este o problemă importantă ce ne preocupă pe toți. Furtul de date a ținut pasul cu dezvoltarea comunicațiilor pe Internet și se folosește de noi metode de a păcăli oamenii să cedeze informațiile private.

Fie că este vorba de adresa e-mail sau de numărul cărții de credit, dacă acestea ajung în mâinile unor persoane nepotrivite vă pot aduce daune: puteți să vă treziți că aveți contul de mail plin de spam sau să constatați cu surprindere că aveți contul bancar golit.

Controlul identității vă protejează împotriva furtului de date confidențiale atunci când sunteți online. Pe baza regulilor create de dumneavoastră, Controlul identității scanează traficul web, e-mail sau de mesagerie instant care iese din calculatorul dumneavoastră în căutare de șiruri de caractere specifice (de exemplu, numărul cardului dumneavoastră de credit). Dacă există o concordanță, site-ul web, e-mailul sau mesajul instant respectiv este blocat.

Puteți crea reguli pentru a proteja orice informație pe care o considerați personală sau confidențială, de la numărul dumneavoastră de telefon sau adresa dumneavoastră de e-mail până la informațiile referitoare la contul dumneavoastră bancar. Este oferit suport pentru mai mulți utilizatori, astfel încât utilizatorii care folosesc alte conturi de utilizator Windows să poată configura și folosi propriile reguli de protecție a identității. Dacă aveți un cont Windows de administrator, regulile pe care le creați pot fi configurate să se aplica și atunci când alți utilizatori ai calculatorului sunt conectați la conturile lor Windows.

De ce să folosiți Controlul identității?

- Controlul identității este foarte eficient în blocarea aplicațiilor spyware keylogger. Acest tip de aplicații malițioase înregistrează tot ceea ce tastezi și trimite aceste înregistrări prin Internet către o persoană malițioasă (un hacker). Hackerul poate afla din datele furate informații confidențiale, cum ar fi parole și numere de conturi bancare, pe care le va folosi în beneficiul propriu.

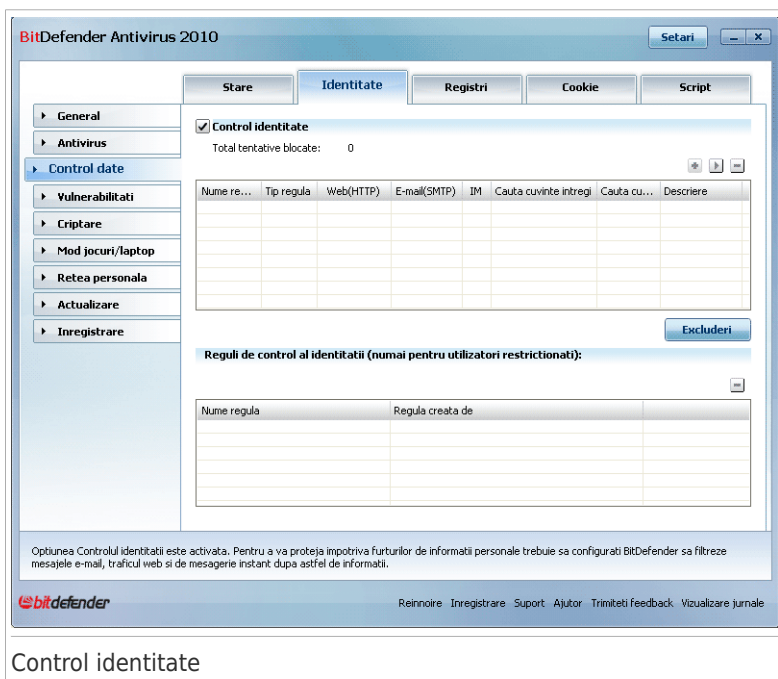
În eventualitatea în care o astfel de aplicație reușește să evite detecția antivirus, aceasta nu va putea trimite datele furate prin e-mail, web sau mesaje instant, dacă ați creat reguli adecvate de protecție a identității.

- Controlul identității vă poate proteja împotriva tentativelor de **phishing** (încercări de a fura informații personale). Cele mai frecvente tentative de phishing utilizează un e-mail înșelător pentru a vă convinge să trimiteți informații personale prin intermediul unei pagini web false.

De exemplu, puteți primi un e-mail care pare a fi trimis de banca dumneavoastră și care vă solicită să actualizați urgent informațiile de cont bancar. E-mailul conține un link către o pagină web unde trebuie să furnizați informațiile personale. Deși par a fi legitime, e-mailul și pagina web spre care vă trimite linkul înșelător sunt false. Dacă faceți clic pe linkul din e-mail și trimiteți informațiile dumneavoastră personale de pe pagina web falsă, veți dezvălui aceste informații persoanelor răuvoitoare care au organizat înșelătoria.

Dacă ați creat reguli adecvate de protecție a identității, nu veți putea trimite informații personale (cum ar fi numărul cărții de credit) de pe o pagină web decât dacă ați definit în mod explicit o excepție pentru pagina web respectivă.

Pentru a configura Controlul identității, mergeți la **Control date personale>Identitate** în Modul Expert.



Dacă doriți să utilizați Controlul identității, urmați acești pași:

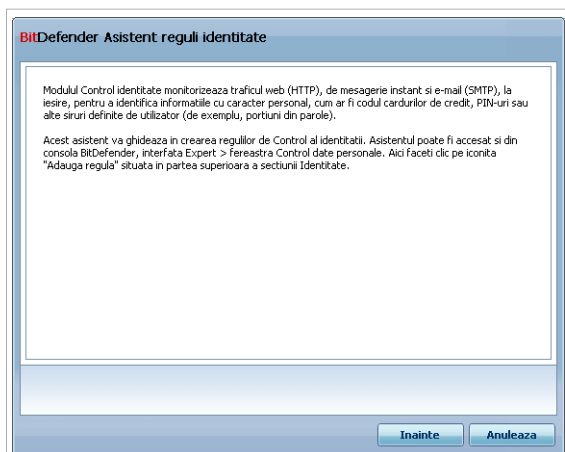
1. Selectați căsuța **Activează Control identitate**.
2. Creați reguli pentru a vă proteja datele confidențiale. Pentru mai multe informații, consultați „*Crearea regulilor de identitate*” (p. 156).
3. Dacă este nevoie, stabiliți anumite excepții la regulile pe care le-ați creat. Pentru mai multe informații, consultați „*Definirea excepțiilor*” (p. 159).
4. Dacă sunteți administratorul sistemului, puteți stabili ca regulile de protecție a identității create de alți administratori să nu se aplice în cazul dvs.

Pentru mai multe informații, consultați „*Regulile stabilite de alți administratori*” (p. 161).

19.2.1. Crearea regulilor de identitate

Pentru a crea o regulă de protecție a identității, faceți clic pe butonul **Adaugă** și urmați pașii programului asistent.

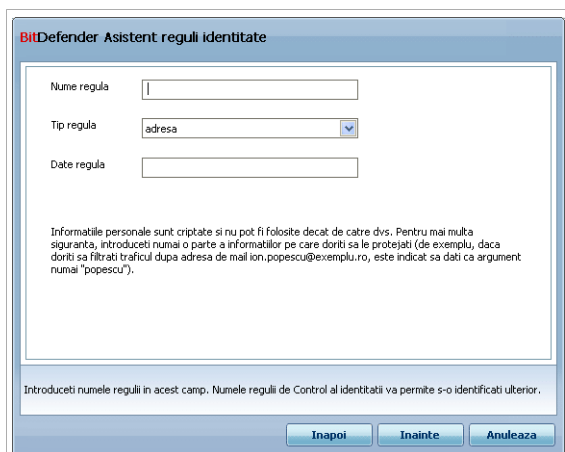
Pasul 1/4 - Fereastra de întâmpinare



Fereastra de întâmpinare

Faceți clic pe **Înainte**.

Pasul 2/4 - Furnizați tipul și argumentul regulei



Furnizați tipul și argumentul regulei

Trebuie setați parametrii următori:

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



Notă

Dacă introduceți mai puțin de trei caractere, vi se va solicita confirmarea acțiunii. Vă recomandăm să introduceți cel puțin trei caractere pentru a evita blocarea greșită a mesajelor și a paginilor web.

Tot ceea ce introduceți este criptat. Pentru mai multă siguranță, nu introduceți întreaga dată pe care vreți să o protejați ci doar o parte a acesteia.

Faceți clic pe **Înainte**.

Pasul 3/4 - Selectați tipuri de trafic și utilizatori

BitDefender Asistent reguli identitate

Protocoloale de scanare:

- Scaneaza traficul web (HTTP)
- Scaneaza traficul e-mail (SMTP)
- Scaneaza mesagerie instant
- Potrivire cuvinte intregi
- Cauta cu majuscule semnificative

Alegeți utilizatorii carora li se va aplica aceasta regula:

- Numai pentru mine (utilizator curent)
- Conturile de utilizatori restrictionati
- Toti utilizatorii

Trafic web (HTTP) si Trafic mesagerie instant care contin informatii personale vor fi blocate.

Selectati aceasta optiune pentru activarea scanarii traficului e-mail (SMTP)

Inapoi Inainte Anuleaza

Selectați tipurile de trafic și utilizatorii

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

- **Scanează web (trafic HTTP)** - scanează traficul HTTP (web) și blochează la ieșire toate datele ce corespund unei reguli.
- **Scanează e-mail (trafic SMTP)** - scanează traficul SMTP (mail) și blochează trimiterea mesajelor e-mail care corespund unei reguli.

- **Scanează MI (mesagerie instant)** - scanează traficul de mesagerie instant și blochează trimiterea mesajelor instant care corespund unei reguli.

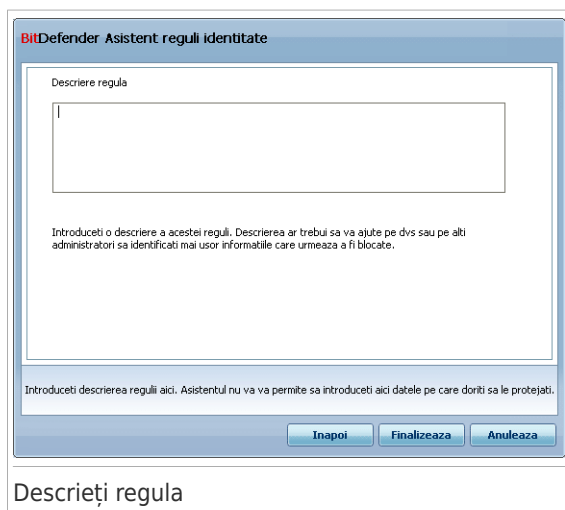
Puteți alege să aplicați regula doar dacă datele protejate apar ca șir independent sau ținând cont de majuscule și minuscule.

Preciați utilizatorii cărora li se aplica regula.

- **Numai mie (utilizator curent)** - regula se va aplica numai contului dvs de utilizator.
- **Conturi utilizatori cu drepturi limitate** - regula se va aplica numai dvs și tuturor conturilor Windows cu drepturi limitate.
- **Toți utilizatorii** - regula se va aplica tuturor conturilor Windows.

Faceți clic pe **Înainte**.

Pasul 4/4 - Descrieți regula



The screenshot shows a dialog box titled "BitDefender Asistent reguli identitate". It contains a text area labeled "Descriere regula" with a cursor. Below the text area is a note: "Introduceți o descriere a acestei reguli. Descrierea ar trebui să vă ajute pe dvs sau pe alți administratori să identificați mai ușor informațiile care urmează să fie blocate." At the bottom of the dialog are three buttons: "Înapoi", "Finalizeaza", and "Anuleaza". Below the dialog box, the text "Descrieți regula" is displayed.

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

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

19.2.2. Definirea excepțiilor

În unele cazuri, este nevoie să definiți excepții pentru anumite reguli de identitate. Considerați cazul în care creați o regulă de identitate care împiedică trimiterea

19.2.3. Administrarea regulilor

Puteți vedea listate în tabel regulile create până în momentul de față.

Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge**.

Pentru a modifica atributele unei reguli, selectați-o și faceți clic pe butonul **Editează** sau faceți dublu-clic pe ea. Va apărea o nouă fereastră.

BITDefender Regula identitate

Nume regula: test

Tip regula: adresa

Date regula: Scrieti aici pentru a schimba

Filtreaza traficul web (HTTP) Potrivire cuvinte intregi

Filtreaza traficul e-mail (SMTP) Cauta cu majuscule semnificative

Filtreaza mesageria instant

Alegeti utilizatorii carora li se va aplica aceasta regula:

Numai pentru mine (utilizator cur) Conturile de utilizatori restrictiati

Toti utilizatorii

Descriere regula

Introduceti numele acestei reguli de Control al identitatii.

OK Anuleaza

Editează regula

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

19.2.4. Reguli stabilite de alți administratori

Dacă nu sunteți singurul utilizator cu drepturi de administrare a sistemului, ceilalți administratori pot crea propriile reguli de identitate. Dacă nu doriți ca regulile create de alți utilizatori să vi se aplice când vă conectați, BitDefender vă permite să stabiliți contul dvs de utilizator ca excepție la respectivele reguli.

Puteți vedea o listă de reguli create de alți administratori în tabelul **Reguli de control al identității**. Tabelul conține numele fiecărei reguli și utilizatorului care a creat-o.

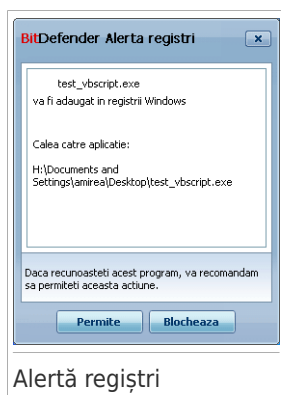
Pentru a vă exclude de la aplicarea unei reguli, selectați regula și faceți clic pe butonul **Șterge**.

19.3. Control regiștri

Una dintre părțile importante ale sistemului de operare Windows sunt **regiștrii**. Aici își păstrează Windows configurația și setările, programele instalate, informații despre utilizator și alte date.

Tot în **regiștri** sunt definite programele care sunt lansate la pornirea Windows. Virușii folosesc des această caracteristică Windows pentru a se lansa automat atunci când utilizatorul își repornește calculatorul.

Controlul Regiștrilor supraveghează regiștrii Windows - în acest fel BitDefender poate detecta troienii. BitDefender vă va alerta de fiecare dată când un program încearcă să modifice informațiile din regiștri astfel încât să fie lansat la pornirea Windows.



Puteți vedea programul care încearcă să modifice regiștrii Windows.

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

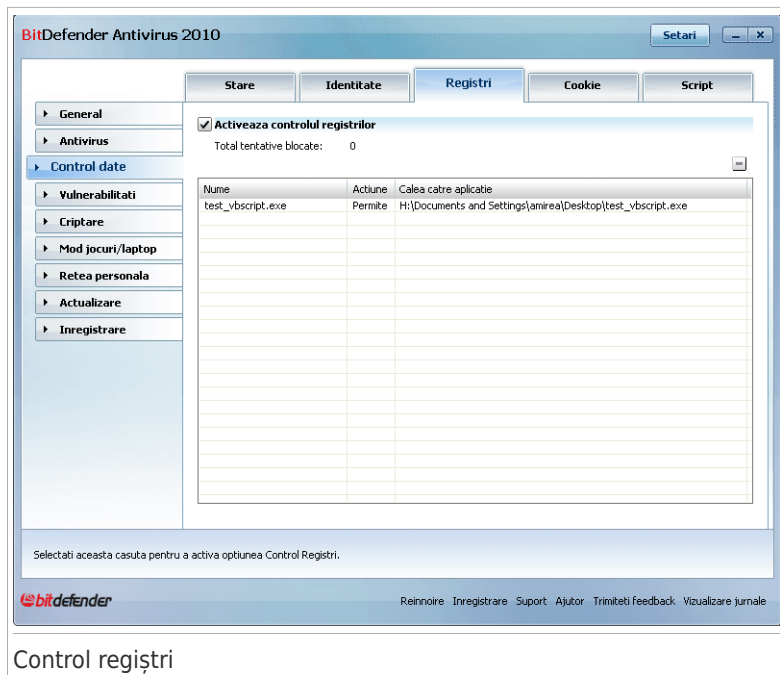
Pe baza răspunsului dumneavoastră, o regulă este creată și listată în tabelul de reguli. Aceeași acțiune este aplicată de fiecare dată când acest program încearcă să modifice o cheie de regiștri.



Notă

BitDefender vă va alerta atunci când instalați programe pentru care este necesară lansarea la pornirea Windows. În cele mai multe cazuri, aceste programe sunt de încredere.

Pentru a configura Controlul identității, mergeți la **Control date personale>Regiștri** în Modul Expert.



Puteți vedea listate în tabel regulile create până în momentul de față.

Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge**.

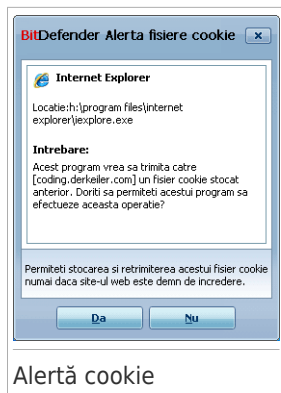
19.4. Controlul fișierelor cookie

Fișierele cookie sunt foarte comune pe Internet. Ele sunt fișiere mici salvate pe calculatorul dumneavoastră. Paginile web creează aceste fișiere pentru a vă monitoriza activitatea pe Internet și a salva informații specifice despre dumneavoastră.

În general, fișierele cookie vă fac viața mai ușoară. De exemplu ele ajută site-urile să vă rețină numele și preferințele, pentru a nu trebui să le introduceți la fiecare vizită.

Dar ele pot fi folosite și pentru a vă compromite intimitatea, urmărindu-vă obiceiurile de navigare pe Internet.

Aici vă ajută **Controlul fișierelor cookie**. Când este activat, **Controlul fișierelor cookie** vă va cere permisiunea de fiecare dată când un site încearcă să seteze un cookie:



Puteți vedea numele aplicației care încearcă să trimită fișierul cookie.

Faceți clic pe **Da** sau pe **Nu** pentru ca o nouă regulă să fie creată, aplicată și menționată în tabelul de reguli.

Aceasta vă va ajuta să alegeți paginile web în care aveți încredere și pe cele în care nu aveți.



Notă

Din cauza numărului mare de fișiere cookie de pe Internet, **Controlul fișierelor cookie** poate fi la început. Inițial, vă va pune foarte multe întrebări despre pagini web care încearcă să seteze cookie-uri pe calculatorul dumneavoastră. După ce adăugați paginile web pe care le folosiți frecvent în lista de reguli, navigarea va deveni la fel de ușoară ca la început.

Pentru a configura Controlul fișierelor cookie, mergeți la **Control date>Cookie** în Modul Expert.

BitDefender Asistent reguli fisiere cookie

Domeniu:

Oricare

Domeniu:

Selectati actiunea

Permite

Interzice

Selectati directia

La iesire

La intrare

Ambele

Selectati site-urile web si domeniile ale caror fisiere cookie sa fie acceptate sau respinse. Fisierile cookie sunt utilizate pentru a monitoriza preferintele dvs pe Internet si alte informatii. Unele pagini nu vor functiona corect fara aceste fisiere.

Selectați adresa, acțiunea și direcția

Puteți seta parametrii:

- **Domeniu** - introduceți adresa domeniului pentru care este creată regula.
- **Acțiune** - selectați acțiunea regulii.

Acțiune	Descriere
Permite	Fișierele cookie ale domeniul respectiv vor fi acceptate.
Interzice	Fișierele cookie ale domeniului respectiv vor fi blocate.

- **Direcție** - selectați direcția traficului.

Tip	Descriere
La ieșire	Regula se aplică numai fișierelor cookie trimise înapoi către siteul de la care au pornit.
La intrare	Regula se aplică numai fișierelor cookie recepționate.
Ambele	Regula se va aplica în ambele direcții.



Notă

Puteți accepta fișiere cookie fără a le returna: setați acțiunea **Interzice** și direcția **La ieșire**.

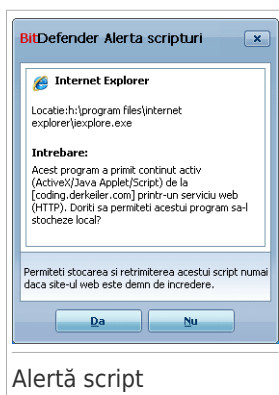
Faceți clic pe **Finalizare**.

19.5. Control scripturi

Scripturile și alte coduri cum ar fi **elementele ActiveX** și **Applet-urile Java**, care sunt folosite pentru a crea pagini web, pot fi programate astfel încât să aibă efecte dăunătoare. Elemente de tipul ActiveX, de exemplu, pot avea în întregime acces la datele dumneavoastră și le pot citi sau șterge de pe calculatorul dumneavoastră, pot captura parole și intercepta mesaje cât timp sunteți conectați la Internet. Este recomandat să acceptați conținutul activ doar de la paginile web pe care le cunoașteți foarte bine și care sunt de încredere.

BitDefender vă permite să alegeți să permiteți sau să blocați execuția acestor elemente.

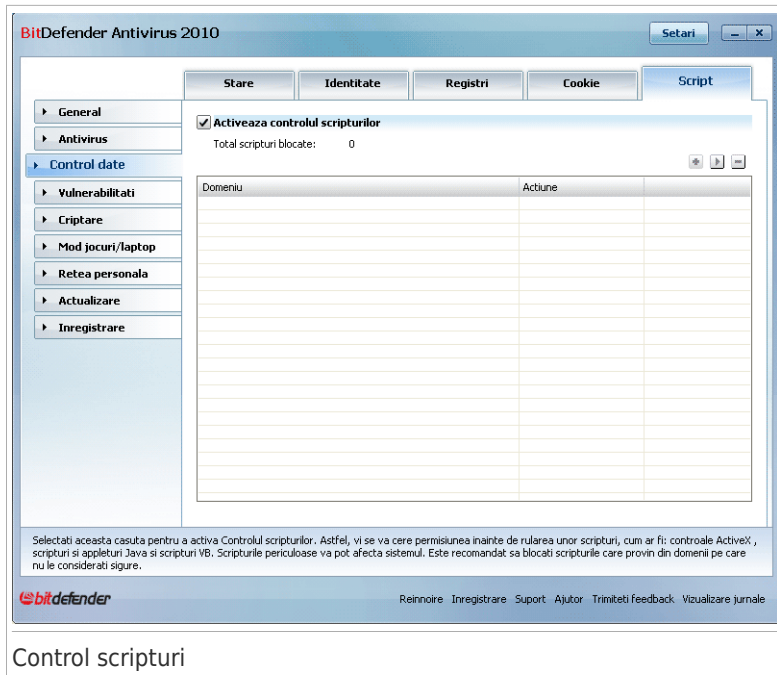
Având **Controlul scripturilor** activat, veți monitoriza adresele web în care aveți încredere și pe cele în care nu aveți. BitDefender vă va cere permisiunea de fiecare dată când un domeniu încearcă să ruleze un script sau alt conținut activ:



Puteți vedea numele resursei.

Faceți clic pe **Da** sau pe **Nu** pentru ca o nouă regulă să fie creată, aplicată și menționată în tabelul de reguli.

Pentru a configura Controlul script-urilor, mergeți la **Control date personale>Script** în Modul Expert.



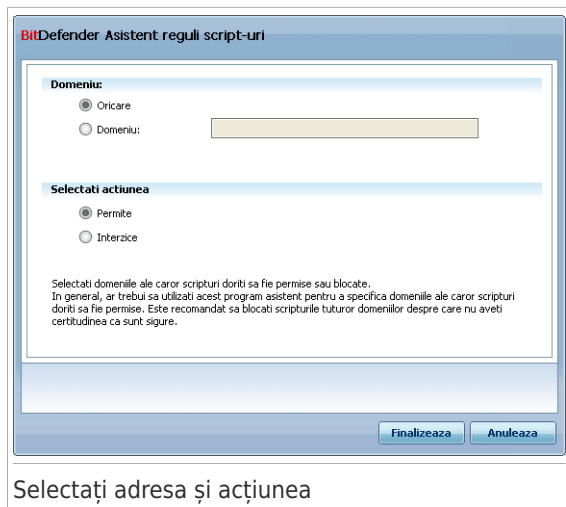
Puteți vedea listate în tabel regulile create până în momentul de față.

Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge**. Pentru a modifica parametrii regulii, selectați regula și faceți clic sau dublu-clic pe butonul **Editează**. Efectuați modificările dorite în fereastra de configurare.

Pentru a crea o regulă manual, faceți clic pe butonul **Adaugă** și configurați parametrii regulii în fereastra de configurare.

19.5.1. Fereastra de configurare

Atunci când editați sau adaugați manual o regulă, va apărea fereastra de configurare.



Puteți seta parametrii:

- **Domeniu** - introduceți adresa domeniului pentru care este creată regula.
- **Acțiune** - selectați acțiunea regulii.

Acțiune	Descriere
Permite	Rularea scripturilor este permisă.
Interzice	Rularea scripturilor este interzisă.

Faceți clic pe **Finalizare**.

20. Vulnerabilitate

Un pas important în protejarea calculatorului dumneavoastră împotriva persoanelor răuvoitoare și a aplicațiilor malițioase este de a menține actualizat sistemul de operare și aplicațiile pe care le utilizați în mod regulat. De asemenea, pentru a preveni accesul fizic neautorizat la calculatorul dumneavoastră, trebuie configurate parole puternice (parole care nu pot fi ghicite cu ușurință) pentru fiecare cont de utilizator Windows.

BitDefender verifică în mod regulat sistemul dumneavoastră în căutare de vulnerabilități și vă informează despre problemele existente.

20.1. Stare

Pentru a configura verificarea automată a vulnerabilităților sau pentru a verifica vulnerabilitățile sistemului, mergeți la **Vulnerabilitate>Stare** în Modul Expert.

BitDefender Antivirus 2010

Stare Setari

Verificarea automată a vulnerabilitatilor este activată

Verifica acum

Stare Verificare vulnerabilitati

Problema	Stare	Actiune
Actualizari Microsoft esentiale	Vechi	Instaleaza
Alte actualizari Microsoft	Cele mai recente	Niciuna
Stare Actualizare automata	Activat	Niciuna
Yahoo! Messenger	Vechi	Detalii
Firefox	Vechi	Detalii
Windows Live Messenger	Vechi	Detalii
amirea	Parola slaba	Remedialaza

Faceti clic aici pentru a administra retea personala.

Reinnoire Inregistrare Suport Ajutor Trimiteți feedback Vizualizare jurnale

Stare vulnerabilități

În tabel sunt afișate problemele identificate în timpul ultimei verificări a gradului de vulnerabilitate și stadiul acestora. Puteți vedea acțiunea pe care trebuie s-o

aplicații pentru a remedia fiecare vulnerabilitate, dacă este cazul. Dacă se indică **Nicio acțiune**, atunci respectiva problemă nu reprezintă o vulnerabilitate.



Important

Pentru a fi informat automat despre vulnerabilitățile sistemului sau aplicațiilor dumneavoastră, mențineți **Verificarea automată a vulnerabilităților** activată.

20.1.1. Remedierea vulnerabilităților

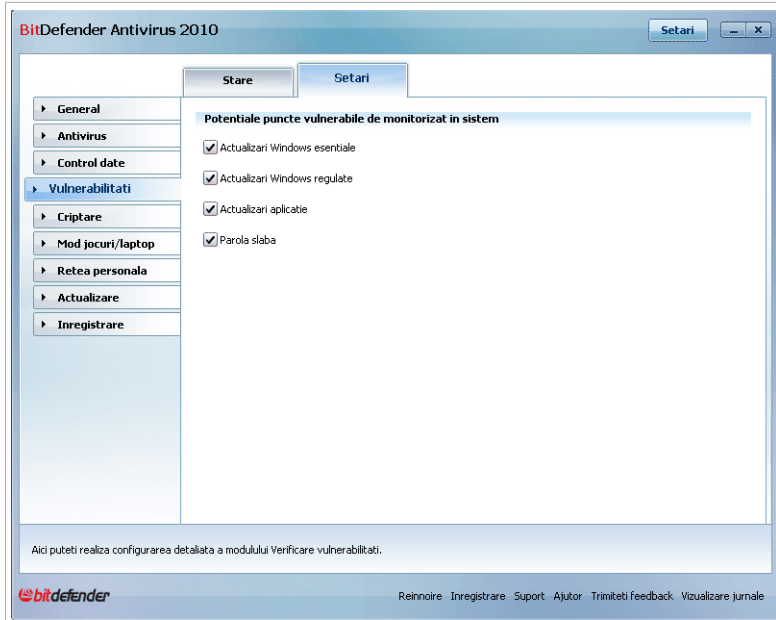
În funcție de problemă, pentru a remedia o anumită vulnerabilitate, procedați după cum urmează:

- Dacă sunt disponibile actualizări Windows, faceți clic pe **Instalează** în coloana **Acțiune** pentru a le instala.
- Dacă există aplicații neactualizate, folosiți linkul **Pagina principală** furnizat, pentru a descărca și instala ultima versiune a respectivei aplicații.
- Dacă un cont de utilizator Windows are o parolă slabă, faceți clic pe **Remediază**, pentru a forța utilizatorul să o modifice la următoarea conectare sau schimbați-o chiar dvs. Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, \$ sau @).

Puteți face clic pe **Verifică acum** și urmați pașii programului asistent pentru a remedia vulnerabilitățile. Pentru mai multe informații, consultați capitolul „*Asistent Verificare vulnerabilități*” (p. 66).

20.2. Setări

Pentru a configura setările verificării automate a vulnerabilităților, mergeți la **Vulnerabilitate>Setări** în Modul Expert.



Setări pentru verificarea automată a vulnerabilităților

Selectați căsuțele corespunzătoare vulnerabilităților care să fie verificate în mod regulat.

- **Actualizări Windows critice**
- **Actualizări Windows obișnuite**
- **Actualizări aplicații**
- **Parole slabe**



Notă

Dacă debifați căsuța corespunzătoare unei anumite vulnerabilități, BitDefender nu vă va mai avertiza despre problemele asociate.

21. 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 și partenerul dumneavoastră de chat, să utilizați fie Yahoo Messenger, fie Windows Live (MSN) Messenger.



Important

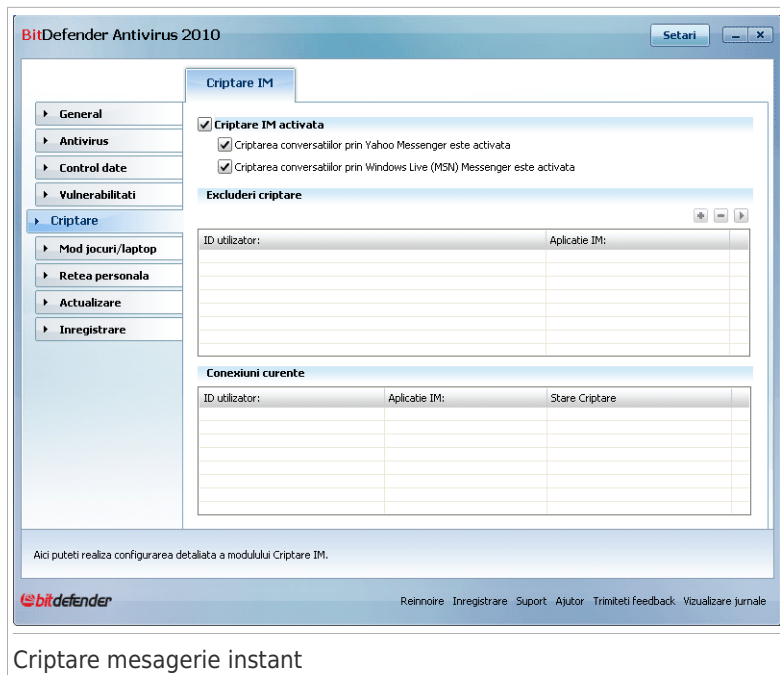
BitDefender nu va cripta o conversație dacă un partener de chat folosește o aplicație web pentru chat, cum ar fi Meebo, sau dacă un partener folosește Yahoo!, iar celălalt Windows Live (MSN).

Pentru a configura criptarea mesageriei instant, mergeți la **Criptare>Criptare MI** în Modul Expert.



Notă

Puteți configura ușor criptarea mesageriei instant folosind bara de comenzi BitDefender din fereastra de chat. Pentru mai multe informații, va rugăm să accesați *„Integrarea în clienți de mesagerie instant”* (p. 206).



Criptare mesagerie instant

Implicit, criptarea mesageriei instant este activată atât pentru Yahoo Messenger, cât și pentru Windows Live (MSN) Messenger. Puteți alege să dezactivați complet criptarea mesageriei instant sau doar pentru o anumită aplicație de chat.

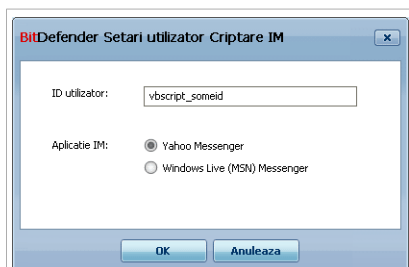
Sunt afișate două tabele:

- **Excluderi criptare** - afișează id-urile de utilizator și programul de mesagerie instant (IM) asociat pentru care criptarea este dezactivată. Pentru a șterge un contact din listă, selectați-l și faceți clic pe butonul **Șterge**.
- **Conexiuni curente** - afișează conexiunile de mesagerie instant curente (ID utilizator și program IM asociat) și dacă aceste conexiuni sunt criptate sau nu. O conexiune poate să nu fie criptată din următoarele motive:
 - ▶ Ați dezactivat în mod explicit criptarea pentru contactul respectiv.
 - ▶ Contactul dumneavoastră nu are instalată o versiune de BitDefender care oferă criptare IM.

21.1. Dezactivarea criptării pentru anumiți utilizatori

Pentru a dezactiva criptarea pentru un anumit utilizator, urmați acești pași:

1. Faceți clic pe butonul **Adaugă** pentru a deschide fereastra de configurare.



Adăugarea contactelor

2. Introduceți în câmpul editabil ID-ul utilizatorului.
3. Selectați aplicația de mesagerie instant asociată contactului.
4. Faceți clic pe **OK**.

22. 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.

22.1. Modul pentru jocuri

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

- Toate alertele și pop-upurile BitDefender sunt dezactivate.
- Nivelul protecției în timp real BitDefender este setat pe **Permisiv**.
- Actualizările nu sunt efectuate în mod implicit.



Notă


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

- Sarcinile de scanare programate sunt dezactivate în mod implicit.

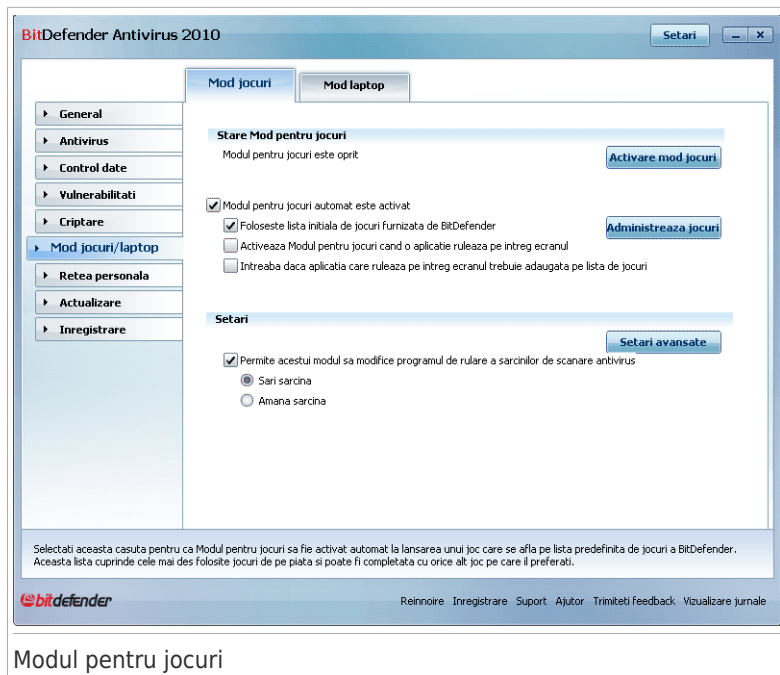
În mod implicit, BitDefender intră automat în modul pentru jocuri când porniți un joc din lista de jocuri cunoscute a BitDefender sau când o aplicație ocupă întreg ecranul (fullscreen). Puteți intra manual în modul pentru jocuri utilizând combinația de taste implicită **Ctrl+Alt+Shift+G**. Este recomandat să ieșiți din modul pentru jocuri atunci când ați terminat jocul (puteți utiliza aceeași combinația de taste implicită **Ctrl+Alt+Shift+G**).



Notă

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

Pentru a configura modul pentru jocuri, mergeți la **Mod jocuri/laptop>Mod jocuri** în modul de vizualizare Expert.



Modul pentru jocuri

În partea de sus a secțiunii, puteți vedea starea modului pentru jocuri. Puteți face clic pe **Intră modul pentru jocuri** sau pe **leși din modul pentru jocuri** pentru a schimba starea curentă.

22.1.1. Configurarea modului pentru jocuri automat

Modul pentru jocuri automat permite BitDefender să intre automat în modul pentru jocuri atunci când este detectat un joc. Puteți configura următoarele opțiuni:

- **Utilizează lista de jocuri furnizată de BitDefender** - pentru a intra automat în modul pentru jocuri când porniți un joc din lista de jocuri cunoscute a BitDefender. Pentru a vedea această listă, faceți clic pe **Administrare jocuri** și apoi pe **Listă jocuri**.
- **Întră în modul pentru jocuri când o aplicație rulează pe ecranul întreg** - pentru a intra automat în Modul pentru jocuri când o aplicație ocupă întregul ecran.
- **Adaugă aplicația pe lista de jocuri?** - pentru a vi se solicita adăugarea unei noi aplicații pe lista de jocuri atunci când aceasta iese din modul ecran întreg. La pornirea unei noi aplicații adăugate pe lista de jocuri, BitDefender va intra automat în modul pentru jocuri.

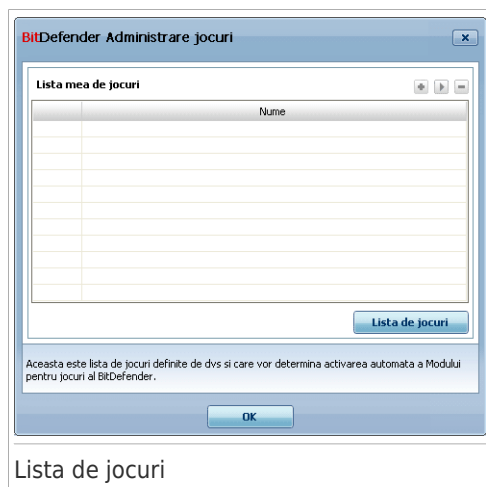


Notă

Dacă nu doriți ca BitDefender să intre automat în modul pentru jocuri, debifați căsuța **Mod automat pentru jocuri**.

22.1.2. Administrarea listei de jocuri

BitDefender intră automat în modul pentru jocuri atunci când porniți o aplicație din lista de jocuri. Pentru a vedea și administra lista de jocuri, faceți clic pe **Administrare jocuri**. Va apărea o nouă fereastră.



Noi aplicații sunt adăugate în această listă când:

- Porniți un joc de pe lista de jocuri cunoscute a BitDefender. Pentru a vedea această listă, faceți clic pe **Listă jocuri**.
- După ieșirea din full screen, adăugați aplicația în lista de jocuri prin intermediul ferestrei de alertă.

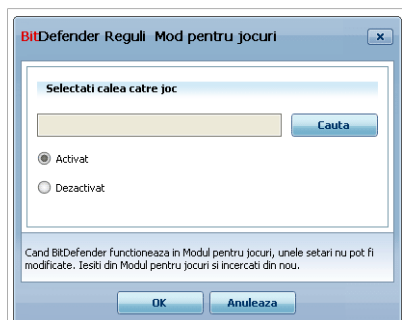
Dacă doriți să dezactivați modul automat pentru jocuri pentru o anumită aplicație din listă, debifați căsuța corespunzătoare acesteia. Puteți dezactiva modul automat pentru jocuri pentru aplicații normale care intră în full screen, cum ar fi browserele web și programele de vizionat filme.

Pentru a administra lista de jocuri, puteți utiliza butoanele plasate în partea de sus a tabelului:

- **Adăugare** - adăugați o nouă aplicație pe lista de jocuri.
- **Eliminare** - eliminați o aplicație de pe lista de jocuri.
- **Editare** - editați un element existent de pe lista de jocuri.

Adăugarea sau editarea jocurilor

Atunci când adăugați sau editați o înregistrare din lista de jocuri, va apărea următoarea fereastră:



Adaugă joc

Faceți clic pe **Caută** pentru a selecta aplicația sau introduceți calea completă către aplicație în câmpul editabil.

Dacă nu doriți ca BitDefender să intre automat în modul pentru jocuri atunci când aplicația selectată este pornită, selectați **Dezactivează**.

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

22.1.3. Configurarea setărilor modului pentru jocuri

Pentru a configura executarea sarcinilor programate, utilizați aceste opțiuni:

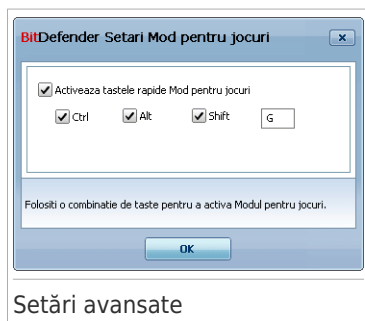
- **Activează acest modul pentru modificarea programelor sarcinilor de scanare antivirus** - pentru a împiedica rularea sarcinilor de scanare programate când Modul pentru jocuri este activat. Puteți selecta una dintre următoarele opțiuni:

Opțiune	Descriere
Sări peste sarcină	Sarcina programată nu este executată deloc.
Amână sarcina	Execută sarcina imediat după ieșirea din modul pentru jocuri.

22.1.4. Schimbarea combinației de taste

Puteți intra manual în modul pentru jocuri utilizând combinația de taste implicită **Ctrl+Alt+Shift+G**. Pentru a schimba combinația de taste, urmați acești pași:

1. Faceți clic pe **Setări avansate**. Va apărea o nouă fereastră.



2. Sub opțiunea **Utilizează combinația de taste**, setați combinația de taste dorită:

- Bifați tastele speciale pe care doriți să le folosiți: tasta Control (Ct r l), tasta Shift (Sh i f t) sau tasta Alternate (A l t).
- În câmpul editabil, tastați litera corespunzătoare tastei normale pe care doriți să o folosiți.

De exemplu, dacă doriți să folosiți combinația de taste Ct r l+A l t+D, trebuie să bifați doar Ct r l și A l t și să tastați D.



Notă

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

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

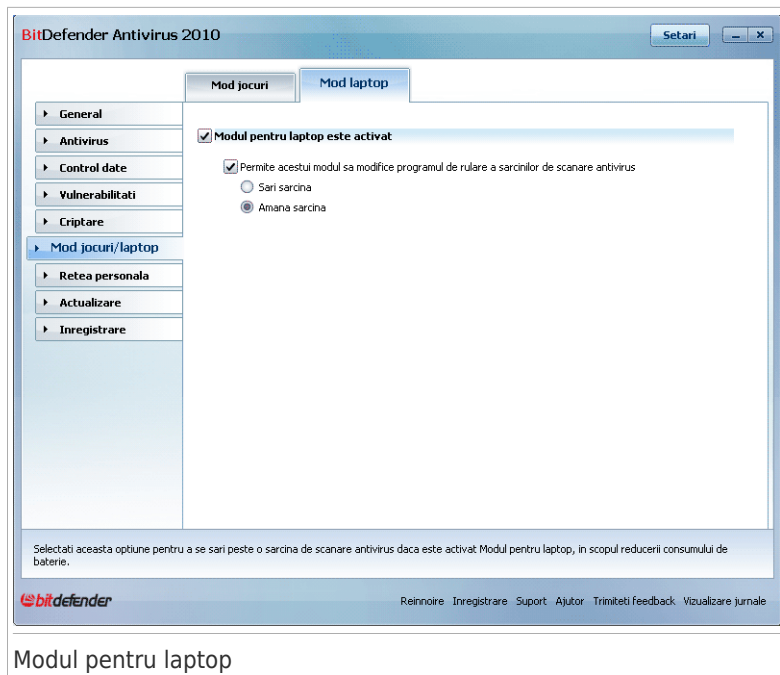
22.2. Modul pentru laptop

Modul pentru laptop este creat special pentru utilizatorii de laptopuri. Scopul acestuia este să minimizeze impactul pe care îl are BitDefender asupra consumului bateriei atunci când aceste dispozitive funcționează pe baterie.

În modul pentru laptop, sarcinile programate nu sunt executate în mod implicit.

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

Pentru a configura modul pentru laptop, mergeți la **Mod jocuri/laptop>Mod laptop** în modul de vizualizare Expert.



Modul pentru laptop

Puteți vedea dacă modul pentru laptop este activat sau nu. Dacă modul pentru laptop este activat, BitDefender va aplica setările configurate atunci când laptopul funcționează pe baterie.

22.2.1. Configurarea setărilor modului pentru laptop

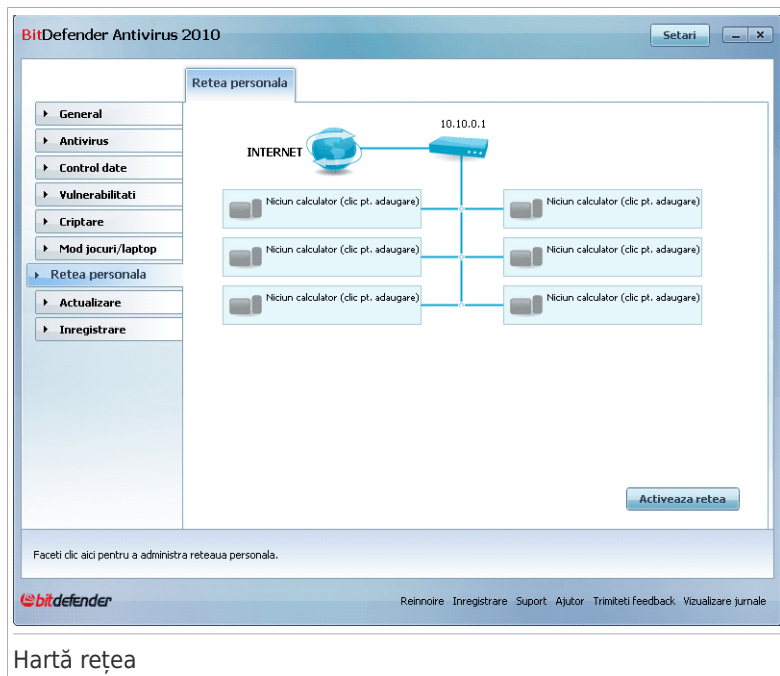
Pentru a configura executarea sarcinilor programate, utilizați aceste opțiuni:

- **Activează acest modul pentru modificarea programelor sarcinilor de scanare antivirus** - pentru a împiedica rularea sarcinilor de scanare programate când Modul pentru laptop este activat. Puteți selecta una dintre următoarele opțiuni:

Opțiune	Descriere
Sări peste sarcină	Sarcina programată nu este executată deloc.
Amână sarcina	Execută sarcina imediat după ieșirea din modul pentru laptop.

23. Rețeaua personală

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



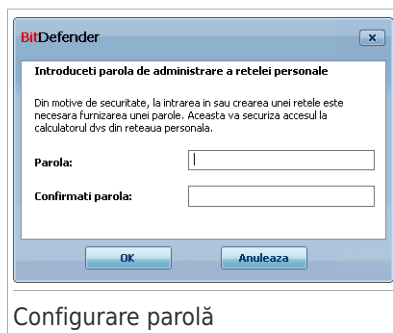
Pentru a putea administra produsele BitDefender instalate pe calculatoarele personale, trebuie să urmați acești pași:

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

23.1. Intrarea în rețeaua BitDefender

Pentru a în rețeaua BitDefender personală, urmați acești pași:

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



The screenshot shows a dialog box titled "BITDefender" with a close button (X) in the top right corner. The main text reads "Introduceți parola de administrare a rețelei personale" (Enter the personal network administration password). Below this, a smaller text block explains: "Din motive de securitate, la intrarea în sau crearea unei rețele este necesară furnizarea unei parole. Această va securiza accesul la calculatorul dvs din rețeaua personală." (For security reasons, when entering or creating a network, it is necessary to provide a password. This will secure access to your computer from the personal network.) There are two input fields: "Parola:" (Password) and "Confirmați parola:" (Confirm password). At the bottom, there are two buttons: "OK" and "Anuleaza" (Cancel).

Configurare parolă

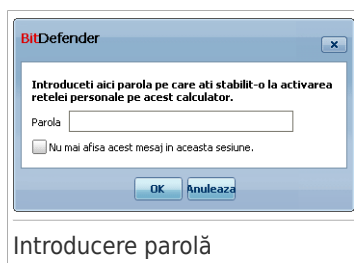
2. Introduceți aceeași parolă în ambele câmpuri editabile.
 3. Faceți clic pe **OK**.
- Puteți vedea numele calculatorului apărând pe harta rețelei.

23.2. Adăugarea calculatoarelor la rețeaua BitDefender

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

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

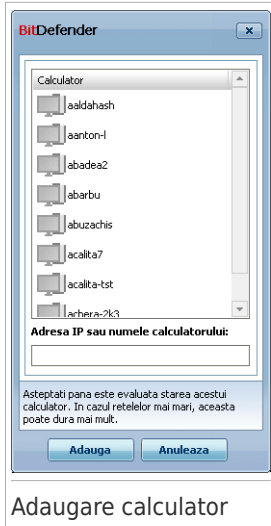
1. Faceți clic pe **Adaugă calculator**. Vi se va cere să furnizați parola locală de administrare a rețelei.



The screenshot shows a dialog box titled "BITDefender" with a close button (X) in the top right corner. The main text reads "Introduceți aici parola pe care ati stabilit-o la activarea rețelei personale pe acest calculator." (Enter here the password you set when activating the personal network on this computer.) There is one input field labeled "Parola" (Password). Below the input field, there is a checkbox with the text "Nu mai afisa acest mesaj in aceasta sesiune." (Do not show this message in this session.). At the bottom, there are two buttons: "OK" and "Anuleaza" (Cancel).




Introducere parolă

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



Adaugare calculator

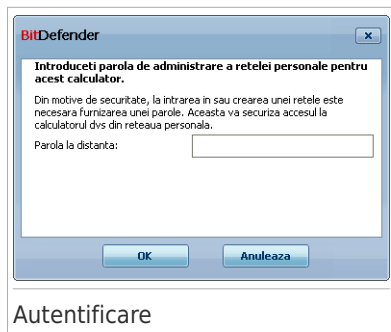
Puteți vedea lista calculatoarelor din rețea. Sensul iconițelor este după cum urmează:

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

3. Puteți proceda astfel:

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

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



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.

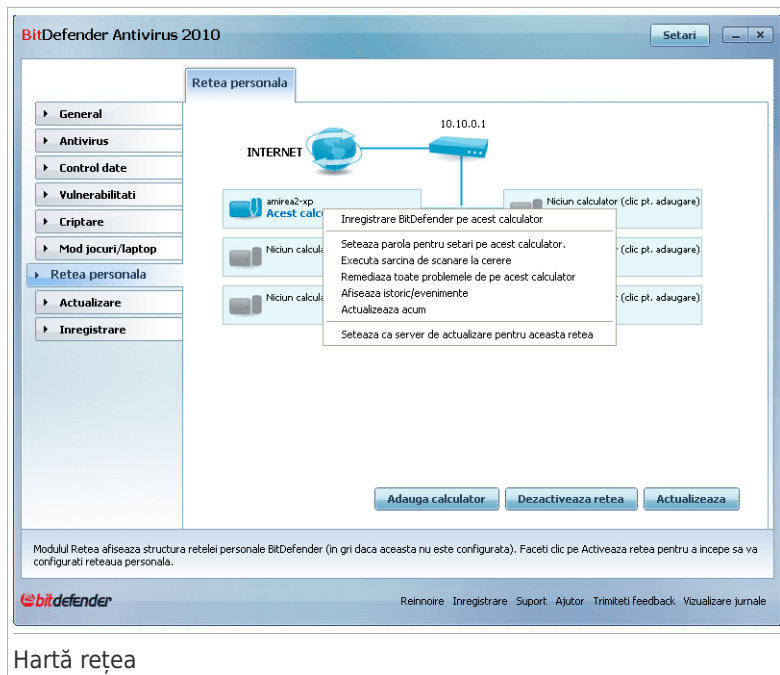


Notă

Puteți adăuga până la cinci calculatoare pe harta rețelei.

23.3. Administrarea rețelei BitDefender

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



Hartă rețea

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

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

● Scoate calculatorul din rețeaua personală

Vă permite să scoateți un calculator din rețea.

● Înregistrează BitDefender pe acest calculator

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

● Stabilește o parolă pentru setări pe un calculator la distanță

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

● Execută o sarcină de scanare la cerere

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

● Remediază toate problemele de pe acest calculator

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

● Vizualizare istoric/evenimente

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

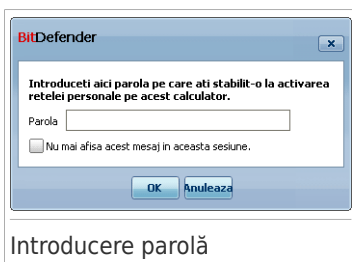
● Update Now

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

● Stabilește acest calculator ca server de actualizare al acestei rețele

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

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



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



Notă

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

24. Actualizare

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

Dacă sunteți conectat la Internet, prin bandă largă sau ADSL, BitDefender se ocupă singur de actualizări. Implicit, BitDefender caută actualizări când deschideți calculatorul și apoi la fiecare **oră**.

Dacă o actualizare este disponibilă, vi se va cere să confirmați actualizarea sau aceasta va fi realizată automat, în funcție de **setările de actualizare automată**.

Procesul de actualizare este realizat progresiv, ceea ce înseamnă că fișierele care trebuie actualizate sunt înlocuite unul câte unul. Astfel, procesul de actualizare nu va afecta funcționarea produsului și, în același timp, orice vulnerabilitate va fi exclusă.

Actualizările sunt de mai multe tipuri:

- **Actualizări pentru motoarele Antivirus** - pentru că apar tot timpul noi viruși, fișierele care conțin semnăturile de viruși trebuiesc actualizate pentru a asigura protecție permanentă, la zi, împotriva acestora. Acest tip de actualizare se mai numește **Actualizare definiții viruși**.
- **Actualizări ale motoarelor antispayware** - se vor adăuga noi semnături de spyware la baza de date. Acest tip de actualizare se mai numește **Actualizare Antispayware**.
- **Actualizare de produs** - la lansarea unei noi versiuni de produs, noi caracteristici și tehnici de scanare sunt introduse pentru a îmbunătăți performanțele produsului. Acest tip de actualizare se mai numește **Upgrade Produs**.

24.1. Actualizarea Automată

Pentru a vedea informații referitoare la actualizare și pentru a iniția actualizări automate, mergeți la **Actualizare>Actualizare** în Modul Expert.

Actualizarea Automată

Aici puteți vedea când au fost realizate ultima căutare de actualizări și ultima actualizare, precum și informații despre ultima actualizare realizată (dacă a fost reușită sau dacă au apărut erori). De asemenea, sunt afișate informații despre versiunea curentă a motorului de scanare și numărul de semnături.

Dacă deschideți această secțiune în timpul unei actualizări, puteți vedea stadiul acesteia.



Important

Pentru a fi protejat împotriva celor mai noi amenințări, mențineți **Actualizarea automată** activată.

24.1.1. Cererea unei actualizări

Actualizarea automată poate fi realizată oricând făcând clic pe **Actualizează acum**. Acest tip de actualizare este cunoscut și ca **actualizare la cererea utilizatorului**.

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



Important

Poate fi necesar ca după realizarea unei actualizări să reporniți calculatorul. Este recomandat să faceți acest lucru cât mai repede posibil.



Notă

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

24.1.2. Dezactivarea actualizării automate

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



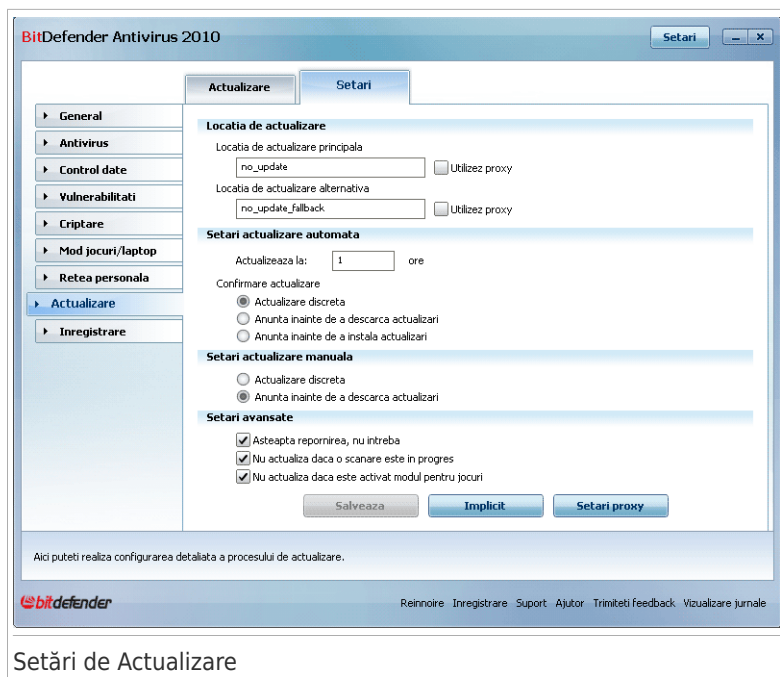
Avertisment

Aceasta este o problemă majoră de securitate. Vă recomandăm să dezactivați actualizarea automată pentru cât mai puțin timp posibil. Dacă nu este actualizat în mod regulat, BitDefender nu va putea să vă protejeze împotriva ultimelor amenințări apărute.

24.2. Setări de Actualizare

Actualizările pot fi realizate din rețeaua locală, de pe Internet, direct sau printr-un server proxy. Implicit, BitDefender va căuta actualizări la fiecare oră, pe Internet, și va instala actualizările disponibile fără a vă mai avertiza.

Pentru a configura setările de actualizare și pentru a administra setările proxy, faceți clic pe **Actualizare>Setări** în Modul Expert.



Setările de actualizare sunt grupate în patru categorii (**Setări locație de actualizare**, **Setări actualizare automată**, **Setări actualizare la cerere** și **Setări avansate**). Fiecare categorie va fi descrisă separat.

24.2.1. Configurarea locațiilor de actualizare

Pentru a seta locațiile de actualizare, utilizați opțiunile din categoria **Setări locație de actualizare**.



Notă

Configurați aceste setări doar dacă sunteți conectat la o rețea locală care stochează local semnături BitDefender de aplicații malițioase sau dacă vă conectați la Internet printr-un server proxy.

Pentru o actualizare mai sigură și mai rapidă, puteți configura două locații de actualizare: o **Locație de actualizare principală** și o **Locație de actualizare alternativă**. Implicit, acestea sunt setate la fel: <http://upgrade.bitdefender.com>.

Pentru a modifica una dintre locațiile de actualizare, introduceți adresa URL a serverului local în câmpul **URL** corespunzător locației pe care doriți să o modificați.



Notă

Vă recomandăm să setați ca locație principală de actualizare serverul local și să lăsați neschimbată adresa locației de actualizare alternative, ca o măsură de siguranță în caz că serverul local devine indisponibil.

În cazul în care compania utilizează un server proxy pentru conectarea la Internet, selectați **Utilizare proxy** și apoi faceți clic pe **Setări proxy** pentru a configura setările proxy. Pentru mai multe informații, consultați „*Administrarea proxy-urilor*” (p. 193).

24.2.2. Configurarea actualizării automate

Pentru a configura procesul de actualizare realizat automat de BitDefender, utilizați opțiunile din categoria **Setări actualizare automată**.

Puteți specifica numărul de ore dintre două căutări consecutive după actualizări în câmpul **Frecvență actualizare**. Intervalul implicit dintre actualizări este de o oră.

Pentru a specifica modul în care să fie realizată actualizarea automată, selectați una dintre următoarele opțiuni:

- **Actualizare discretă** - BitDefender descarcă și realizează actualizarea automat.
- **Anunță înainte de a descărca actualizări** - de fiecare dată când o actualizare este disponibilă, veți fi anunțat înainte de a o descărca.
- **Anunță înainte de a instala actualizări** - de fiecare dată când o actualizare a fost descărcată, veți fi anunțat înainte de a o instala.

24.2.3. 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.

24.2.4. Configurarea setărilor avansate

Pentru ca procesul de actualizare al BitDefender să nu vă afecteze munca, configurați opțiunile din categoria **Setări avansate**:

- **Nu cere restart pentru actualizare** - Dacă o actualizare necesită repornirea sistemului, produsul își va continua funcționarea folosind fișierele vechi până când utilizatorul va reporni calculatorul din proprie inițiativă. Utilizatorului nu i se va cere repornirea calculatorului și astfel actualizarea BitDefender nu va interfera cu activitatea utilizatorului.

- **Nu actualiza dacă o scanare este în progres** - BitDefender nu se va actualiza dacă o scanare este în desfășurare. Astfel, procesul de actualizare BitDefender nu va interfera cu sarcinile de scanare.



Notă

Dacă BitDefender este actualizat în timpul unei scanări, procesul de scanare va fi anulat.

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

24.2.5. Administrarea proxy-urilor

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



Notă

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

Pentru a administra setările proxy, faceți clic pe **Setări proxy** . Va apărea o nouă fereastră.

BitDefender Setari proxy

Proxy detectat la momentul instalarii

Adresa: Port: Nume utilizator:
Parola:

Proxy browser implicit

Adresa: Port: Nume utilizator:
Parola:

Proxy personalizat

Adresa: Port: Nume utilizator:
Parola:

Aici puteti modifica setarile de proxy detectate la momentul instalarii.

OK Anuleaza

Fereastra de gestionare a setărilor proxy

Există trei seturi de setări proxy:

- **Proxy detectat la instalare** - setări proxy detectate pe contul administratorului în timpul instalării și care pot fi configurate doar dacă sunteți conectat la acel cont. Dacă serverul proxy necesită un nume de utilizator și o parolă pentru autentificare, atunci va trebui să le specificați în câmpurile corespunzătoare.
- **Browser proxy implicit** - setări proxy ale utilizatorului curent, extrase din browserul implicit. Dacă serverul proxy solicită un nume de utilizator și o parolă pentru autentificare, specificați-le în câmpurile corespunzătoare.



Notă

Browserele web suportate sunt Internet Explorer, Mozilla Firefox și Opera. Dacă utilizați un alt browser în mod implicit, BitDefender nu va putea obține setările proxy ale utilizatorului curent.

- **Personalizare proxy** - setări proxy pe care le puteți configura dacă sunteți autentificat ca administrator.

Următoarele setări trebuie specificate:

- ▶ **Adresă** - introduceți adresa IP a serverului proxy.
- ▶ **Port** - introduceți portul folosit BitDefender pentru a se conecta la serverul proxy.
- ▶ **Utilizator** - introduceți un nume de utilizator recunoscut de proxy.
- ▶ **Parolă** - introduceți o parolă validă pentru numele de utilizator introdus.

Atunci când BitDefender va încerca să se conecteze la Internet, va fi încercat pe rând fiecare set de setări proxy, până când se va reuși conexiunea.

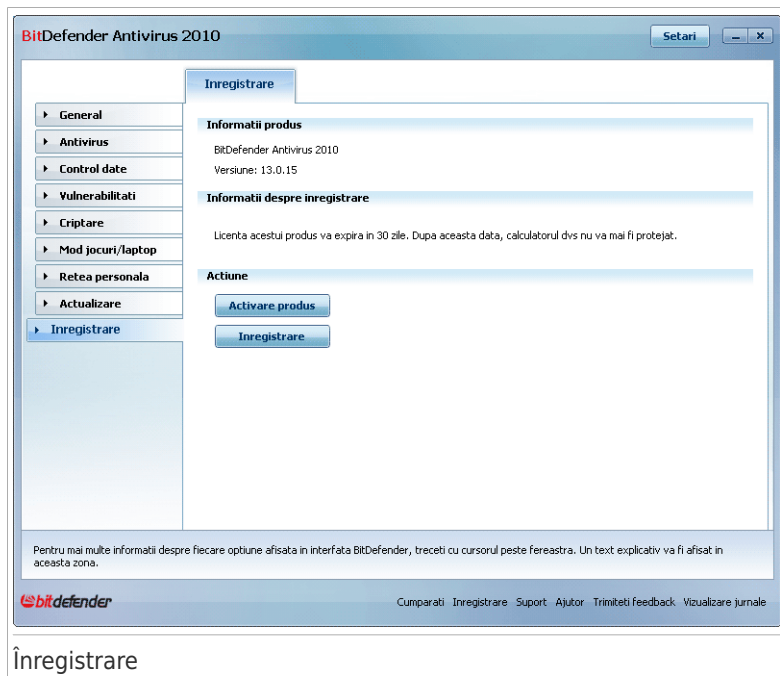
Mai întâi, va fi utilizat setul conținând propriile dumneavoastră setări proxy pentru conectarea la Internet. Dacă acesta nu merge, vor fi încercate în continuare setările proxy detectate la instalare. În sfârșit, dacă nici acestea nu sunt bune, vor fi extrase setările proxy ale utilizatorului curent din browserul implicit și vor fi folosite pentru conectarea la Internet.

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

Faceți clic pe **Aplică** pentru a salva schimbările sau pe **Implicit** pentru a încărca setările standard.

25. Înregistrare

Pentru a afla informații complete despre produsul dumneavoastră BitDefender și despre stadiul înregistrării, mergeți la **Înregistrare** în Modul Expert.



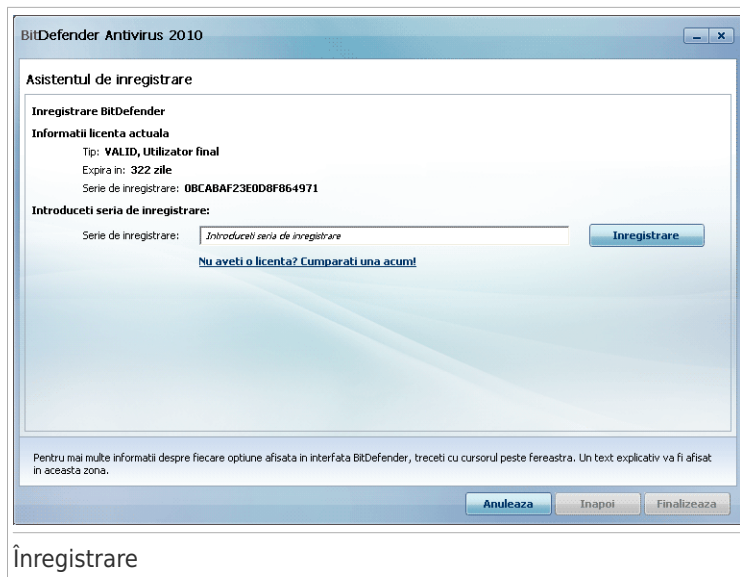
Înregistrare

Această secțiune afișează:

- **Informații despre produs:** produsul BitDefender și versiunea acestuia.
- **Informații despre înregistrare:** adresa de e-mail utilizată pentru a vă conecta la contul dumneavoastră BitDefender (dacă a fost configurată), seria curentă de înregistrare și câte zile au mai rămas până la expirarea licenței.

25.1. Înregistrarea BitDefender Antivirus 2010

Faceți clic pe **Înregistrare** pentru a deschide fereastra de înregistrare a produsului.



Înregistrare

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

Pentru a înregistra BitDefender Antivirus 2010:

1. Introduceți seria de înregistrare în câmpul editabil.



Notă

Puteți găsi seria dumneavoastră de înregistrare:

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

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

2. Faceți clic pe **Înregistrare**.

3. Faceți clic pe **Finalizare**.

25.2. Crearea unui cont BitDefender

În cadrul procesului de înregistrare, ESTE NECESAR să vă creați un cont BitDefender. Contul BitDefender vă oferă acces la actualizări BitDefender, suport tehnic gratuit, oferte speciale și promoții. Dacă v-ați pierdut seria de înregistrare BitDefender,

puteți accesa contul dumneavoastră la <http://myaccount.bitdefender.com> pentru a o recupera.



Important

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

Dacă nu ați creat încă un cont BitDefender, faceți clic pe **Activează cont** pentru a deschide fereastra de înregistrare a contului.

BitDefender Antivirus 2010

Asistentul de înregistrare

Cont BitDefender

Pentru a avea acces la actualizări automatizate și la suport tehnic, activați BitDefender prin crearea/accesarea unui cont. Activarea poate fi amânată 15 zile pentru versiunile de evaluare și 30 de zile pentru versiunile înregistrate. Mai multe informații la http://www.bitdefender.com/why_register.

Creeaza cont nou

Adresa de e-mail:

Parola: Confirmati parola:

Optiuni e-mail:

Acceseaza cont creat anterior

Amana inregistrarea (inregistrarea este obligatorie)

Pentru mai multe informatii despre fiecare optiune afisata in interfata BitDefender, treceti cu cursorul peste fereastra. Un text explicativ va fi afisat in aceasta zona.

Creare cont

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

- „Nu am un cont BitDefender” (p. 197)
- „Deja am un cont BitDefender” (p. 198)

Nu am un cont BitDefender

Pentru a crea un cont BitDefender, urmați acești pași:

1. Selectați **Creează cont nou**.

2. Introduceți informațiile solicitate în câmpurile corespunzătoare. Informațiile furnizate aici vor rămâne confidențiale.

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



Notă

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

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

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

4. Faceți clic pe **Creează**.

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

6. **Activați-vă contul**. Pentru a vă putea utiliza contul, trebuie mai întâi să îl activați. Verificați-vă adresa de e-mail și urmați instrucțiunile din mesajul trimis de către serviciul de înregistrare BitDefender.

Deja am un cont BitDefender

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

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

1. Selectați **Accesează cont creat anterior**.

2. Introduceți adresa de e-mail și parola contului dvs în câmpurile corespunzătoare.



Notă

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

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

- **Vreau sa primesc toate mesajele**

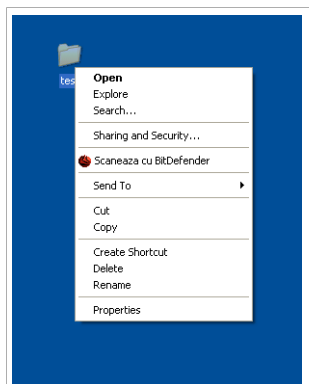
- **Vreau sa primesc numai mesaje despre produs**
- **Nu vreau sa primesc niciun mesaj**

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

Integrarea în Windows și în aplicațiile terților

26. Integrarea în meniul contextual Windows

Meniul contextual Windows apare atunci când faceți clic-dreapta pe un fișier sau pe un director de pe calculator sau pe obiectele de pe desktop.



Meniul contextual Windows

BitDefender se integrează în meniul contextual Windows pentru a vă ajuta să scanați rapid fișiere după viruși. Puteți găsi rapid opțiunea BitDefender în meniul contextual uitându-vă după iconița BitDefender.

26.1. Scanează cu BitDefender

Utilizând meniul contextual Windows, puteți scana cu ușurință fișiere, directoare și chiar partiții întregi. Faceți clic-dreapta pe obiectul pe care doriți să-l scanați și selectați **Scanează cu BitDefender** din meniu. Va apărea **programul asistent de scanare** care vă va ghida de-a lungul procesului de scanare.

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

Dacă doriți să modificați opțiunile de scanare, urmați acești pași:

1. Deschideți BitDefender și treceți interfața în Modul Expert.
2. Faceți clic pe **Antivirus** în meniul din stânga.
3. Faceți clic pe tabul **Scanare viruși**.
4. Faceți clic-dreapta pe sarcina **Scanare contextuală** și selectați **Deschide**. Va apărea o fereastră.

5. Faceți clic pe **Personalizat** și configurați opțiunile de scanare după cum este necesar. Pentru a afla ce face o opțiune, țineți mouse-ul deasupra ei și citiți descrierea afișată în partea de jos a ferestrei.
6. Faceți clic pe **OK** pentru a salva modificările.
7. Faceți clic pe **OK** pentru a confirma și aplica noile opțiuni de scanare.



Important

Este recomandat să nu modificați opțiunile de scanare ale acestei metode de scanare decât dacă aveți un motiv anume să faceți acest lucru.


27. Integrarea cu browserele web

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

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

- Internet Explorer
- Mozilla Firefox

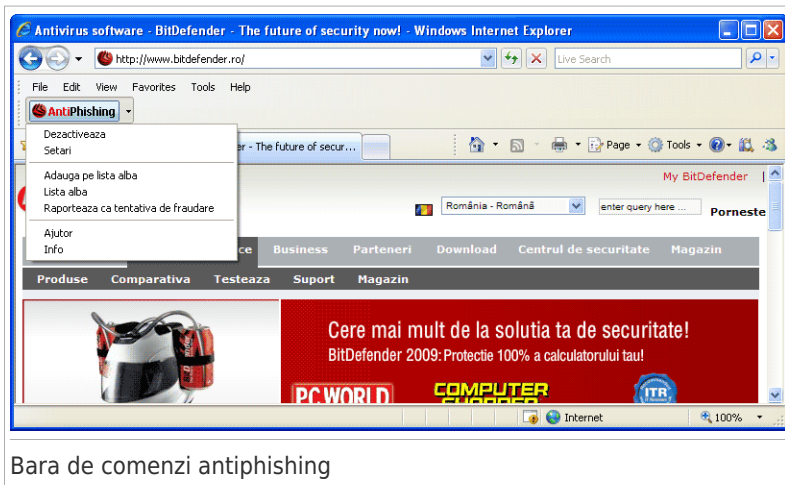
Puteți administra ușor și eficient protecția antiphishing și lista albă utilizând bara de comenzi BitDefender Antiphishing integrată în browserele web de mai sus.

Bara de comenzi antiphishing, reprezentată prin  iconița BitDefender se află în zona de sus a browserului. Faceți clic pe ea pentru a deschide meniul barei de instrumente.



Notă

Dacă nu puteți vedea bara de instrumente, deschideți meniul **View**, mergeți cu cursorul pe **Toolbars** și bifați **BitDefender Toolbar**.



Bara de comenzi antiphishing

Următoarele comenzi sunt disponibile pe meniul barei de instrumente:

- **Activează / Dezactivează** - activează / dezactivează protecția antiphishing BitDefender în browserul web curent.

- **Setări** - deschide o fereastră în care puteți specifica setările barei de comenzi antiphishing. Următoarele opțiuni sunt disponibile:
 - ▶ **Protecția antiphishing pentru web în timp real** - detectează și vă avertizează în timp real dacă un site web este folosit pentru a fura informații personale. Această opțiune controlează protecția antiphishing oferită de BitDefender doar pentru browserul web curent.
 - ▶ **Întreabă înainte de a adăuga în lista albă** - vă avertizează înainte de a adăuga o pagină web în lista albă.
- **Adaugă pe lista albă** - adaugă pagina web curentă în lista albă.



Notă

Adăugarea unei pagini web în lista albă înseamnă că BitDefender nu o va mai scana după amenințări phishing. Vă recomandăm să adăugați în lista albă doar paginile web în care aveți deplină încredere.

- **Lista albă** - deschide lista albă.



Lista albă antiphishing

Puteți vedea lista tuturor paginilor web care nu sunt verificate de motoarele antiphishing ale BitDefender. Dacă doriți să ștergeți o pagină web din lista albă, astfel încât să fiți avertizat în legătură cu orice amenințare phishing existentă pe pagina respectivă, faceți clic pe butonul **Șterge** corespunzător paginii.

Puteți adăuga paginile web în care aveți deplină încredere pe lista albă pentru a nu mai fi scanate de motoarele antiphishing. Pentru a adăuga o pagină web pe lista albă, introduceți adresa acesteia în câmpul corespunzător și faceți clic pe **Adaugă**.

- **Raportează ca fraudat (phishing)** - informează laboratorul BitDefender că site-ul web respectiv este folosit pentru furt de informații personale. Raportând site-urile web folosite pentru fraudă, ajutați la protejarea altor persoane împotriva furtului de identitate.
- **Ajutor** - deschide documentația electronică.
- **Despre** - deschide o fereastră în care puteți vedea informații despre BitDefender și unde să apelați pentru ajutor în cazul unei probleme.

28. Integrarea în clienți de mesagerie instant

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

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

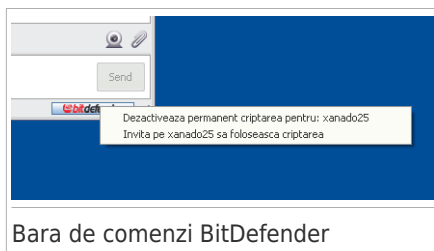
- Partenerul dumneavoastră de chat are instalată o versiune de BitDefender care suportă criptarea mesageriei instant (IM), iar Criptarea IM este activată pentru aplicația de mesagerie instant folosită pentru chat.
- Atât dumneavoastră, cât și partenerul dumneavoastră de chat, să utilizați fie Yahoo Messenger,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



Important

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

Puteți configura ușor criptarea mesageriei instant folosind bara de comenzi BitDefender din fereastra de chat. Bara de comenzi se găsește în mod normal în colțul din dreapta-jos al ferestrei de chat. Uitați-vă după logo-ul BitDefender pentru a o găsi.



Notă

Bara de comenzi arată când o conversație este criptată prin afișarea unei cheițe 🔑 lângă logo-ul BitDefender.

Făcând clic pe bara de comenzi BitDefender, vă sunt oferite următoarele opțiuni:

- **Dezactivează permanent criptarea pentru contact.**
- **Invită pe contact să utilizeze criptarea.** Pentru a cripta conversația, contactul dumneavoastră trebuie să instaleze BitDefender și să utilizeze un program de mesagerie instant compatibil.

Ghid de instrucțiuni

29. Cum scanați fișiere și directoare

Scanarea cu BitDefender este ușoară și flexibilă. Sunt 4 metode de a seta BitDefender să scaneze fișiere și directoare după viruși și alte aplicații malițioase:

- Utilizând meniul contextual Windows
- Utilizând sarcini de scanare
- Utilizând opțiunea Scanare manuală BitDefender
- Utilizând bara de scanare

Imediat ce ați inițiat o scanare, va apărea programul asistent de scanare care vă va ghida de-a lungul acestui proces. Pentru informații detaliate despre acest program asistent, consultați secțiunea „*Programul asistent de scanare*” (p. 54).

29.1. Utilizând meniul contextual Windows

Aceasta este metoda cea mai ușoară și recomandată pentru a scana un fișier sau un director de pe calculatorul dumneavoastră. Faceți clic-dreapta pe obiectul pe care doriți să-l scanați și selectați **Scanează cu BitDefender** din meniu. Urmați programul asistent de scanare pentru a finaliza scanarea.

Iată câteva situații în care este recomandată folosirea acestei metode de scanare:

- Suspectați un anumit fișier sau director că este infectat.
- Atunci când descărcați de pe Internet fișiere care credeți că ar putea fi periculoase.
- Scanați un director comun din rețea înainte de a copia fișiere din acesta pe calculatorul dumneavoastră.

29.2. Utilizând sarcini de scanare

Dacă doriți să vă scanați calculatorul sau anumite directoare în mod regulat, este indicat să utilizați sarcini de scanare. Sarcinile de scanare specifică locațiile care trebuie scanate de BitDefender, precum și opțiunile de scanare și acțiunile care trebuie aplicate. În plus, aveți posibilitatea să le **programați** pentru a fi executate în mod regulat sau la o anumită oră.


Pentru a vă scana calculatorul utilizând sarcini de scanare, trebuie să deschideți BitDefender și să rulați sarcina de scanare dorită. Pașii de urmat pentru rularea sarcinii de scanare variază în funcție de modul de vizualizare a interfeței cu utilizatorul.

Rularea sarcinilor de scanare în Modul Novice

În Modul Novice, puteți rula numai scanarea standard a întregului sistem, dacă faceți clic pe **Scanează acum**. Urmați programul asistent de scanare pentru a finaliza scanarea.

Rularea sarcinilor de scanare în Modul Intermediar

În Modul Intermediar puteți rula o serie de sarcini de scanare preconfigurate. De asemenea, puteți configura și rula sarcini de scanare personalizate în anumite locații de pe calculatorul dvs, folosind opțiunile de scanare personalizată. Urmați acești pași pentru a rula o sarcină de scanare în Modul Intermediar:

1. Faceți clic pe tabul **Antivirus**.
2. În partea stângă a zonei Sarcini rapide, faceți clic pe **Scanare de sistem** pentru a lansa o scanare standard a întregului calculator. Pentru a rula o altă sarcină de scanare, faceți clic pe săgeata  de pe buton și selectați sarcina de scanare dorită. Pentru a configura și executa o scanare personalizată, faceți clic pe **Scanare personalizată**. Acestea sunt sarcinile de scanare disponibile:

Sarcină de scanare	Descriere
Scanare de sistem	Scanează întregul sistem, cu excepția arhivelor. În configurația implicită, scanează după toate tipurile de aplicații periculoase, altele decât cele de tip rootkit .
Scanare profundă sistem	Scanează întregul sistem. În configurația implicită, se scanează după toate tipurile de aplicații malițioase care amenință securitatea sistemului dumneavoastră, cum ar fi virușii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) și altele.
Scanează documente	Utilizați această sarcină pentru a scana directoare importante ale utilizatorului curent: My Documents, Desktop și StartUp. Astfel, veți asigura siguranța documentelor dumneavoastră, un spațiu de lucru sigur și rularea la pornirea sistemului a unor aplicații necompromise.
Scanare personalizată	Această opțiune vă ajută să configurați și să rulați o sarcină de scanare personalizată, permițându-vă să specificați obiectele de scanat și opțiunile generale de scanare. Puteți salva sarcini de scanare personalizată pentru a le putea accesa ulterior în Modul Intermediar sau Expert.

3. Urmați programul asistent de scanare pentru a finaliza scanarea. Dacă ați ales să efectuați o scanare personalizată, trebuie să parcurgeți programul Asistent scanare personalizată.

Rularea sarcinilor de scanare în Modul Expert

În Modul Expert, puteți rula toate sarcinile de scanare preconfigurate și, de asemenea, puteți schimba opțiunile lor de scanare. În plus, puteți crea sarcini de scanare personalizate pentru a scana anumite locații de pe calculator. Urmați acești pași pentru a rula o sarcină de scanare în Modul Expert:

1. Faceți clic pe **Antivirus** în meniul din stânga.
2. Faceți clic pe tabul **Scanare viruși**. Aici găsiți o serie de sarcini de scanare standard și puteți crea propriile sarcini de scanare. Acestea sunt sarcinile de scanare standard pe care le puteți utiliza:


Sarcină implicită	Descriere
Scanare profundă sistem	Scanează întregul sistem. În configurația implicită, se scanează după toate tipurile de aplicații malițioase care amenință securitatea sistemului dumneavoastră, cum ar fi virușii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) și altele.
Scanare de sistem	Scanează întregul sistem, cu excepția arhivelor. În configurația implicită, scanează după toate tipurile de aplicații periculoase, altele decât cele de tip rootkit .
Scanare rapidă sistem	Scanează directoarele Windows și Program Files. În configurația implicită, se scanează după toate tipurile de aplicații malițioase, mai puțin cele ascunse (rootkituri), dar nu sunt scanate memoria, regiștrii și fișierele cookie.
Documentele mele	Utilizați această sarcină pentru a scana directoare importante ale utilizatorului curent: My Documents, Desktop și StartUp. Astfel, veți asigura siguranța documentelor dumneavoastră, un spațiu de lucru sigur și rularea la pornirea sistemului a unor aplicații necompromise.

3. Faceți dublu-clic pe sarcina de scanare pe care doriți să o rulați.
4. Urmați programul asistent de scanare pentru a finaliza scanarea.

29.3. Utilizând opțiunea Scanare manuală BitDefender

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

Pentru a vă scana calculatorul utilizând opțiunea Scanare manuală BitDefender, urmați acești pași:

1. Pe meniul Windows Start , urmați calea **Start → Programs → BitDefender 2010 → Scanare manuală BitDefender**. Va apărea o nouă fereastră.
2. Faceți clic pe **Adaugă director** pentru a selecta ținta scanării. Va apărea o nouă fereastră.
3. Selectați locația de scanat:
 - Pentru a vă scana desktopul, selectați **Desktop**.
 - Pentru a scana o partiție de hard-disk, selectați partiția respectivă din My Computer.
 - Pentru a scana un anumit director, căutați și selectați directorul respectiv.
4. Faceți clic pe **OK**.
5. Faceți clic pe **Continue** pentru a începe scanarea.
6. Urmăriți programul asistent de scanare pentru a finaliza scanarea.

Ce este Safe Mode?

Safe Mode este un mod special de a porni Windows, utilizat în principal pentru a depana problemele care afectează funcționarea normală a Windows. Aceste probleme variază de la conflicte provocate de drivere până la viruși care împiedică pornirea normală a Windows. În Safe Mode, Windows încarcă doar un minim de componente ale sistemului de operare și drivere de bază. Doar câteva aplicații funcționează în Safe Mode. Acesta este motivul pentru care majoritatea virușilor sunt inactivi și pot fi ușor eliminați atunci când Windows operează în Safe Mode.

Pentru a porni Windows în Safe Mode, reporniți calculatorul și apăsați tasta F8 încontinuu până apare meniul de opțiuni avansate al Windows (Windows Advanced Options Menu). Puteți alege între mai multe opțiuni de a porni Windows în Safe Mode. Este recomandat să selectați **Safe Mode with Networking** pentru a avea acces la Internet.



Notă

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

29.4. Utilizarea barei de scanare

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

Puteți utiliza bara de scanare pentru a scana rapid fișiere și directoare. Trageți fișierul sau directorul care doriți să fie scanat peste bara de scanare. Urmați programul asistent de scanare pentru a finaliza scanarea.



Notă

Pentru mai multe informații, consultați secțiunea „*Bara de scanare*” (p. 32).

30. Cum să programați scanarea calculatorului

Este recomandat să vă scanați calculatorul periodic pentru a-l proteja de viruși. BitDefender vă permite să programați sarcini de scanare, astfel încât să vă puteți scana automat calculatorul.

Pentru a programa BitDefender să vă scaneze calculatorul, urmați acești pași:

1. Deschideți BitDefender și treceți interfața în Modul Expert.
2. Faceți clic pe **Antivirus** în meniul din stânga.
3. Faceți clic pe tabul **Scanare viruși**. Aici găsiți o serie de sarcini de scanare standard și puteți crea propriile sarcini de scanare.
 - Sarcinile de sistem sunt disponibile și pot fi rulate pe orice cont de utilizator Windows.
 - Sarcinile de utilizator sunt disponibile și pot fi rulate numai de către utilizatorul care le-a creat.

Acestea sunt sarcinile de scanare standard pe care le puteți programa:

Sarcină implicită	Descriere
Scanare profundă sistem	Scanează întregul sistem. În configurația implicită, se scanează după toate tipurile de aplicații malițioase care amenință securitatea sistemului dumneavoastră, cum ar fi virușii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) și altele.
Scanare de sistem	Scanează întregul sistem, cu excepția arhivelor. În configurația implicită, scanează după toate tipurile de aplicații periculoase, altele decât cele de tip rootkit .
Scanare rapidă sistem	Scanează directoarele Windows și Program Files. În configurația implicită, se scanează după toate tipurile de aplicații malițioase, mai puțin cele ascunse (rootkituri), dar nu sunt scanate memoria, registrul și fișierele cookie.
Scanare autologon	Scanează obiectele executate atunci când un utilizator se conectează la Windows. Pentru a utiliza această sarcină, trebuie să o programați să ruleze la pornirea sistemului. În mod implicit, scanarea autologon este dezactivată.

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

Dacă niciuna dintre aceste sarcini de scanare nu este potrivită scopului dumneavoastră, puteți crea o nouă sarcină de scanare, pe care o puteți programa apoi pentru a rula după cum este necesar.

4. Faceți clic-dreapta pe sarcina de scanare dorită și selectați **Planifică**. Va apărea o nouă fereastră.
5. Programați sarcina să ruleze după cum este necesar:
 - Pentru a rula sarcina de scanare o singură dată, selectați **O singură dată** și specificați data și ora începerii.
 - Pentru a rula sarcina de scanare la pornirea sistemului, selectați **La pornirea sistemului**. Puteți indica după cât timp de la pornirea sistemului să fie rulată sarcina (în minute).
 - Pentru a rula sarcina de scanare periodic, selectați **Periodic** și specificați cât de des să ruleze, precum și data și ora începerii.



Notă

De exemplu, pentru a vă scana calculatorul în fiecare sâmbătă, la ora 2 dimineața, trebuie să configurați programul după cum urmează:

- a. Selectați **Periodic**.
 - b. În câmpul **La fiecare**, tastați **1** și apoi selectați **săptămâni** din meniu. În acest fel, sarcina este rulată o dată pe săptămână.
 - c. Setati ca dată de început următoarea zi de sâmbătă.
 - d. Setati ora începerii la **2 : 00 : 00**.
6. Faceți clic pe **OK** pentru a salva programul. Sarcina de scanare va rula în mod automat conform programului pe care l-ați definit. Dacă aveți calculatorul închis atunci când sarcina trebuie să ruleze, aceasta va fi executată imediat ce deschideți calculatorul.

Remedierea problemelor și asistența

31. Remedierea problemelor

Acest capitol prezintă unele probleme care pot apărea atunci când folosiți BitDefender și vă oferă soluții posibile. Majoritatea acestor probleme pot fi remediate prin configurarea adecvată a setărilor de produs.

Dacă problema dvs nu este prezentată aici sau dacă soluțiile oferite nu vă sunt de ajutor, puteți contacta echipa de suport tehnic BitDefender folosind informațiile din capitolul „Suport” (p. 221).

31.1. Probleme la instalare

Acest articol vă ajută să remediați problemele care apar cel mai des la instalarea BitDefender. Aceste probleme pot face parte din următoarele categorii:

- **Erori de validare a instalării:** asistentul de instalare nu pot fi rulat din cauza unei anumite situații a sistemului dvs.
- **Instalări eșuate:** ați inițiat instalarea din asistentul de instalare, dar procesul nu s-a finalizat.

31.1.1. Erori de validare a instalării

Când porniți asistentul de instalare, sunt verificate o serie de condiții pentru validarea necesară inițierii instalării. În tabelul de mai jos sunt prezentate cel mai des întâlnite erori de validare a instalării și soluțiile pentru remedierea lor.

Eroare	Descriere & Soluție
Nu aveți drepturile necesare pentru instalarea programului.	<p>Pentru a rula asistentul de instalare și pentru a instala BitDefender, aveți nevoie de drepturi de administrator. Puteți proceda în oricare dintre următoarele modalități:</p> <ul style="list-style-type: none"> ● Conectați-vă la un cont Windows de administrator și rulați din nou asistentul de instalare. ● Faceți clic-dreapta pe fișierul de instalare și selectați Rulează ca. Introduceți numele de utilizator și parola corespunzătoare unui cont Windows de administrator al sistemului.
Programul de instalare a detectat o versiune anterioară BitDefender, care nu a fost deinstalată corect.	<p>BitDefender a fost instalat anterior pe sistemul dvs, dar versiunea respectivă nu a fost deinstalată complet. Acest fapt împiedică instalarea unei noi versiuni BitDefender.</p> <p>Pentru a remedia această eroare și pentru a instala BitDefender, urmați acești pași:</p>

Eroare	Descriere & Soluție
	<ol style="list-style-type: none"> 1. Mergeți la www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dvs. 2. Rulați instrumentul de dezinstalare folosind drepturile de administrare a sistemului. 3. Reporniți calculatorul. 4. Reporniți asistentul de instalare BitDefender.
<p>Produsul BitDefender nu este compatibil cu sistemul dvs de operare.</p>	<p>Încercați să instalați BitDefender pe un sistem de operare cu care acesta nu este compatibil. Consultați „<i>Cerințe de sistem</i>” (p. 2) pentru a afla care sunt sistemele de operare care permit instalarea BitDefender.</p> <p>Dacă sistemul dvs de operare este Windows XP cu Service Pack 1 sau fără nici un pachet de servicii, puteți să instalați Service Pack 2 sau mai recent și apoi să rulați din nou asistentul de instalare.</p>
<p>Fișierul de instalare este proiectat pentru un alt tip de procesor.</p>	<p>Dacă obțineți o astfel de eroare, înseamnă că încercați să rulați o versiune incorectă a fișierului de instalare. Există două versiuni ale fișierului de instalare BitDefender: una pentru procesoare pe 32 de biți și cealaltă pentru procesoare pe 64 de biți.</p> <p>Pentru a vă asigura că aveți versiunea corectă pentru sistemul dvs, descărcați fișierul de instalare direct de la www.bitdefender.com.</p>

31.1.2. Instalare eșuată

Există mai multe cauze posibile ale unei instalări eșuate:

- În timpul instalării apare un ecran de eroare. Vi se poate solicita să anulați instalarea sau vi se poate pune la dispoziție un buton prin care să rulați un instrument de dezinstalare, care va curăța sistemul.



Notă

Imediat după inițierea instalării BitDefender, puteți fi informat că nu există suficient spațiu liber pe disc. În acest caz, eliberați spațiul necesar pe partiția pe care doriți să instalați BitDefender și apoi reluați sau reinițiați instalarea.

- Instalarea nu înaintează și, eventual, sistemul se blochează. Sistemul reacționează numai după repornire.

- Instalarea s-a finalizat, dar nu puteți folosi funcțiile BitDefender, parțial sau în totalitate.

Pentru a reuși instalarea BitDefender după o tentativă eșuată, urmați acești pași:

1. **Curățați sistemul după instalarea eșuată.** Dacă instalarea eșuează, unele chei de regiștri și fișiere BitDefender pot rămâne în sistemul dvs. Aceste rămășițe pot împiedica instalarea ulterioară a BitDefender. De asemenea, ele pot afecta funcționarea și stabilitatea sistemului. De aceea, este necesar să le ștergeți înainte de a încerca să reinstalați produsul.

Dacă pe ecranul de eroare apare un buton de rulare a unui instrument de deinstalare, faceți clic pe el pentru a curăța sistemul. În caz contrar, procedați după cum urmează:

- a. Mergeți la www.bitdefender.com/uninstall și descărcați instrumentul de deinstalare pe calculatorul dvs.
 - b. Rulați instrumentul de deinstalare folosind drepturile de administrare a sistemului.
 - c. Reporniți calculatorul.
2. **Verificați cauzele posibile ale instalării eșuate.** Înainte de a începe reinstalarea produsului, verificați dacă există și eliminați posibilele cauze ale instalării inițiale eșuate:
 - a. Verificați dacă aveți instalată orice altă soluție de securitate pentru că ea ar putea perturba funcționarea normală a BitDefender. Vă recomandăm să deinstalați toate celelalte soluții de securitate și apoi să reinstalați BitDefender.
 - b. De asemenea, este recomandat să verificați dacă sistemul dvs este infectat. Puteți proceda în oricare dintre următoarele modalități:
 - Folosiți CD-ul BitDefender de repornire în situații de urgență (rescue CD) și eliminați orice pericol existent. Pentru mai multe informații, consultați capitolul „*BitDefender Rescue CD*” (p. 224).
 - Deschideți o fereastră Internet Explorer, mergeți la www.bitdefender.com și efectuați o scanare online (faceți clic pe butonul **Scanare online**).
 3. Încercați din nou să instalați BitDefender. Este recomandat să descărcați și să rulați cea mai recentă versiune a fișierului de instalare de pe www.bitdefender.ro.
 4. Dacă instalarea eșuează, vă rugăm să contactați BitDefender pentru suport, folosind informațiile din secțiunea „*Support*” (p. 221).

31.2. Serviciile BitDefender nu răspund

Acest articol vă ajută să remediați problema *Serviciile BitDefender nu răspund*. Această problemă poate apărea în următoarele situații:

- Iconița BitDefender din **bara de sistem** apare în gri și o fereastră pop-up vă informează că serviciile BitDefender nu răspund.
- Fereastra BitDefender indică faptul că serviciile BitDefender nu răspund.

Problema poate fi cauzată de:

- o actualizare importantă este în curs de instalare.
- erori temporare de comunicare între serviciile BitDefender.
- unele dintre serviciile BitDefender sunt oprite.
- alte soluții de securitate rulează pe calculatorul dvs, în același timp cu BitDefender.
- viruși de pe sistemul dvs afectează funcționarea normală a BitDefender.

Pentru a remedia această problemă, încercați următoarele soluții:

1. Așteptați câteva momente pentru a vedea dacă apar schimbări. Eroarea poate fi temporară.
2. Reporniți calculatorul și așteptați câteva momente până când se încarcă BitDefender. Deschideți BitDefender pentru a vedea dacă eroarea persistă. De obicei, repornirea calculatorului rezolvă problema.
3. Verificați dacă aveți instalată orice altă soluție de securitate pentru că ea ar putea perturba funcționarea normală a BitDefender. Vă recomandăm să dezinstalați toate celelalte soluții de securitate și apoi să reinstalați BitDefender.
4. Dacă eroarea persistă, este posibil să existe o problemă mai gravă (de exemplu, calculatorul dvs ar putea fi infectat cu un virus care afectează funcționarea BitDefender). Vă rugăm să contactați BitDefender pentru suport, folosind informațiile din secțiunea „*Support*” (p. 221).

31.3. Nu s-a reușit dezinstalarea BitDefender

Acest articol vă ajută să remediați erorile care pot apărea la dezinstalarea BitDefender. Sunt posibile două situații:

- În timpul dezinstalării apare un ecran de eroare. Ecranul oferă un buton pentru rularea unui instrument de dezinstalare, care va curăța sistemul.
- Dezinstalarea nu înaintează și, eventual, sistemul se blochează. Faceți clic pe **Anulare** pentru a abandona dezinstalarea. Dacă anularea nu este posibilă, reporniți sistemul.

Dacă dezinstalarea eșuează, unele chei de regiștri și fișiere BitDefender pot rămâne în sistemul dvs. Aceste rămășițe pot împiedica instalarea ulterioară a BitDefender. De asemenea, ele pot afecta funcționarea și stabilitatea sistemului. Pentru a dezinstala BitDefender complet de pe sistemul dvs, trebuie să rulați instrumentul de dezinstalare.

Dacă dezinstalarea nu reușește și se afișează un ecran de eroare, faceți clic pe butonul de rulare a instrumentul de dezinstalare, pentru a curăța sistemul. În caz contrar, procedați după cum urmează:

1. Mergeți la www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dvs.
2. Rulați instrumentul de dezinstalare folosind drepturile de administrare a sistemului. Utilitarul de dezinstalare va șterge toate fișierele și cheile din regiștri care nu au fost șterse în timpul procesului automatizat de dezinstalare.
3. Reporniți calculatorul.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru suport, conform descrierii din secțiunea „*Support*” (p. 221).

32. Suport

BitDefender se străduiește să ofere clienților săi un nivel cât mai ridicat în ceea ce privește rapiditatea și calitatea suportului tehnic. BitDefender Knowledge Base (<http://www.bitdefender.ro/suport>) furnizează articole care conțin soluții la majoritatea problemelor și întrebărilor dumneavoastră legate de BitDefender. Dacă nu găsiți soluția în Knowledge Base, puteți contacta echipa de suport tehnic a BitDefender. Reprezentanții BitDefender vă vor răspunde la întrebări în timp util și vă vor oferi toată asistența de care aveți nevoie.

32.1. BitDefender Knowledge Base

BitDefender Knowledge Base este o bază online de informații despre produsele BitDefender. Stochează, într-un format accesibil, rapoarte ale echipelor de suport și dezvoltare cu privire la rezultatele suportului tehnic continuu și ale activităților de eliminare a bug-urilor BitDefender împreună cu articole mai generale despre prevenția virușilor, administrarea soluțiilor BitDefender și explicații detaliate, și multe alte articole.

BitDefender Knowledge Base este pusă la dispoziția publicului. Această multitudine de informații reprezintă încă o cale de a oferi clienților BitDefender asistența tehnică de care au nevoie. Toate cererile valide de informații sau rapoarte despre bug-uri venind de la clienții BitDefender ajung în cele din urmă în BitDefender Knowledge Base, ca rapoarte asupra eliminării bug-urilor, fișe de lucru sau articole informative pentru a suplimenta fișierele de suport ale produsului.

BitDefender Knowledge Base este disponibilă oricând la adresa <http://kb.bitdefender.ro>.

32.2. Solicitarea ajutorului

Puteți cere ajutor prin intermediul serviciului online de asistență al BitDefender. Uрмаți pașii de mai jos:

1. Mergeți la <http://www.bitdefender.ro/suport>. Aici se află BitDefender Knowledge Base. BitDefender Knowledge Base oferă numeroase articole care conțin soluții la probleme legate de utilizarea soluțiilor BitDefender.
2. Căutați în BitDefender Knowledge Base articole care vă pot ajuta să rezolvați problema pe care o întâmpinați.
3. Vă rugăm să citiți articolul relevant și să încercați soluția propusă.
4. Dacă soluția respectivă nu vă rezolvă problema, folosiți linkul din articol pentru a contacta echipa de suport tehnic a BitDefender.
5. Intrați în contul dumneavoastră BitDefender.
6. Contactați reprezentanții BitDefender prin e-mail, pe chat sau la telefon.

32.3. Informații de contact

Comunicarea eficientă este cheia unei afaceri de succes. În ultimii 10 ani BitDefender a câștigat o reputație indisputabilă în depășirea așteptărilor clienților și partenerilor, căutând în mod constant mijloace pentru o comunicare eficientă. Nu ezitați să ne contactați indiferent ce problemă sau întrebare ați avea.

32.3.1. Adrese Web

Departament de vânzări: sales@bitdefender.ro
Suport tehnic: kb.bitdefender.ro
Documentație: documentation@bitdefender.com
Programe de Parteneriat: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Relații Media: pr@bitdefender.com
Carriere: jobs@bitdefender.com
Subscrieri viruși: virus_submission@bitdefender.com
Subscrieri spam: spam_submission@bitdefender.com
Raportare abuz: abuse@bitdefender.com
Site produs: <http://www.bitdefender.ro>
Arhive ftp ale produsului: <ftp://ftp.bitdefender.com/pub>
Distribuitori locali: <http://www.bitdefender.ro/site/Partnership/list/>
BitDefender Knowledge Base: <http://kb.bitdefender.ro>

32.3.2. Filialele BitDefender

Sucursalele BitDefender sunt pregătite să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și pe cele generale. Adresele lor precum și modul în care pot fi contactate sunt date mai jos.

Romania

BITDEFENDER SRL

West Gate Park, Building H2, 24 Preciziei Street
Bucharest

Fax: +40 21 2641799

Telefon vânzări: +40 21 2063470

E-mail vânzări: sales@bitdefender.ro

Suport tehnic: <http://www.bitdefender.ro/suport>

Site web: <http://www.bitdefender.ro>

U.S.A

BitDefender, LLC

6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309

Telefon (birou&vânzări): 1-954-776-6262
Vânzări: sales@bitdefender.com
Suport tehnic: <http://www.bitdefender.com/help>
Web: <http://www.bitdefender.com>

Germany

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Birou: +49 2301 91 84 222
Vânzări: vertrieb@bitdefender.de
Suport tehnic: <http://kb.bitdefender.de>
Web: <http://www.bitdefender.de>

Marea Britanie și Irlanda

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
E-mail: info@bitdefender.co.uk
Telefon: +44 (0) 8451-305096
Vânzări: sales@bitdefender.co.uk
Suport tehnic: <http://www.bitdefender.com/help>
Web: <http://www.bitdefender.co.uk>

Spain

BitDefender España SLU
C/ Balmes, 191, 2º, 1ª, 08006
Barcelona
Fax: +34 932179128
Telefon: +34 902190765
Vânzări: comercial@bitdefender.es
Suport tehnic: www.bitdefender.es/ayuda
Site web: <http://www.bitdefender.es>

BitDefender Rescue CD

33. Descriere generală

BitDefender Antivirus 2010 este furnizat cu un CD de boot (BitDefender Rescue CD) capabil a scana și dezinfecă tot calculatorul fără a fi necesară pornirea sistemului de operare.

Este indicat să utilizați BitDefender Rescue CD oricând sistemul dumneavoastră de operare nu funcționează corect din cauza infecției cu viruși. Aceasta se întâmplă în general când nu folosiți un produs antivirus.

Actualizarea definițiilor de viruși se face automat, fără intervenția utilizatorului de fiecare dată când este pornit BitDefender Rescue CD.

BitDefender Rescue CD este o distribuție Knoppix adaptată de BitDefender, care integrează cea mai recentă soluție de securitate BitDefender pentru Linux într-un CD GNU/Linux Knoppix Live, oferind un antivirus pentru desktop care este capabil să scaneze și să dezinfecă hard discurile existente (incluzând partițiile Windows NTFS). De asemenea, BitDefender Rescue CD poate fi utilizat pentru a restaura datele dumneavoastră importante atunci când nu puteți porni Windowsul.



Notă

BitDefender Rescue CD poate fi descărcat de la această locație:
http://download.bitdefender.com/rescue_cd/

33.1. Cerințe de sistem

Înainte de a porni BitDefender Rescue CD, trebuie să vă asigurați că sistemul dumneavoastră îndeplinește următoarele cerințe.

Tip procesor

Procesor compatibil cu x86, minimum 166 MHz, dar nu așteptați performanțe ridicate în acest caz. Un procesor de generație i686, la 800MHz, constituie o alegere mai bună.

Memorie

Minimum 512 MB memorie RAM (1 GB recomandat)

CD-ROM

BitDefender Rescue CD rulează de pe un CD-ROM, de aceea sunt necesare un CD-ROM și un BIOS capabil să-l pornească.

Conexiune Internet

Deși BitDefender Rescue CD va rula fără conexiune Internet, procedurile de actualizare vor necesita un link HTTP activ, chiar și printr-un server proxy. De aceea, pentru o protecție actualizată, conexiunea Internet este o CERINȚĂ.

Rezoluție grafică

Placă video standard compatibilă SVGA.

33.2. Soft inclus

BitDefender Rescue CD include următoarele pachete soft.

Xedit

Acesta este un editor text de fișiere.

Vim

Acesta este un editor text de fișiere avansat, oferind evidențierea sintaxei, o interfață grafică și multe altele. Pentru mai multe informații, consultați [pagina web a Vim](#).

Xcalc

Acesta este un calculator.

RoxFiler

RoxFiler este manager de fișiere grafic, rapid și avansat.

Pentru mai multe informații, consultați [pagina web a RoxFiler](#).

MidnightCommander

GNU Midnight Commander (mc) este un manager de fișiere în mod text.

Pentru mai multe informații, consultați [pagina web a MC](#).

Pstree

Pstree afișează procesele care rulează.

Top

Top afișează sarcinile Linux.

Xkill

Xkill oprește un program care rulează în X.

Partition Image

Partition Image vă ajută să salvați partiții în format EXT2, Reiserfs, NTFS, HPFS, FAT16 și FAT32 într-un fișier imagine. Acest program poate fi util în scopuri de backup.

Pentru mai multe informații, consultați [pagina web a Partimage](#).

GtkRecover

GtkRecover este o versiune GTK a programului de recuperare de consolă. Vă ajută să recuperați un fișier.

Pentru mai multe informații, consultați [pagina web a GtkRecover](#).

ChkRootKit

ChkRootKit este un utilitar care vă ajută să vă scanați calculatorul după rootkituri.

Pentru mai multe informații, consultați [pagina web a ChkRootKit](#).

Nessus Network Scanner

Nessus este un scanner de securitate remote pentru Linux, Solaris, FreeBSD și Mac OS X.

Pentru mai multe informații, consultați [pagina web a Nessus](#).

Iptraf

Iptraf este un soft de monitorizare de rețea.

Pentru mai multe informații, consultați [pagina web a Iptraf](#).

Iftop

Iftop afișează consumul de lățime de bandă pe o interfață.

Pentru mai multe informații, consultați [pagina web a Iftop](#).

MTR

MTR este un utilitar de analiză de rețea.

Pentru mai multe informații, consultați [pagina web a MTR](#).

PPPStatus

PPPStatus afișează statistici referitoare la traficul TCP/IP la intrare și la ieșire.

Pentru mai multe informații, consultați [pagina web a PPPStatus](#).

Wavemon

Wavemon este o aplicație de monitorizare a dispozitivelor de rețea wireless.

Pentru mai multe informații, consultați [pagina web a Wavemon](#).

USBView

USBView afișează informații despre dispozitivele conectate la magistrala USB.

Pentru mai multe informații, consultați [pagina web a USBView](#).

Pppconfig

Pppconfig vă ajută să configurați automat o conexiune ppp prin dial-up.

DSL/PPPoE

DSL/PPPoE configurează o conexiune PPPoE (ADSL).

I810rotate

I810rotate activează ieșirea video pe hardware i810 utilizând i810switch(1).

Pentru mai multe informații, consultați [pagina web a I810rotate](#).

Mutt

Mutt este un client de mail MIME avansat, cu interfață text.

Pentru mai multe informații, consultați [pagina web a Mutt](#).

Mozilla Firefox

Mozilla Firefox este un browser web foarte popular.

Pentru mai multe informații, consultați [pagina web a Mozilla Firefox](#).

Elinks

Elinks un browser web în mod text.

Pentru mai multe informații, consultați [pagina web a Elinks](#).

34. Instrucțiuni BitDefender Rescue CD

Acest capitol conține informații despre pornirea și oprirea BitDefender Rescue CD, scanarea calculatorului dumneavoastră după aplicații malițioase precum și salvarea datelor de pe un PC cu Windows compromis pe un dispozitiv mobil. Totuși, utilizând aplicațiile software care sunt oferite pe CD, puteți executa numeroase alte sarcini, descrierea acestora fiind departe de scopul acestui manual de utilizare.

34.1. Pornirea BitDefender Rescue CD

Pentru a porni cd-ul, setați BIOS-ul calculatorului dumneavoastră să demareze de pe cd, așezați cd-ul în drive și reporniți calculatorul. Asigurați-vă că poate fi pornit calculatorul dumneavoastră de pe cd.

Așteptați până apare următorul ecran și urmați instrucțiunile pentru a porni BitDefender Rescue CD.



Ecran la pornirea sistemului

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

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



Desktopul

34.2. 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.

```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufs) (aufs) (aufs) (aufs)
ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksuspend)
) (aio/0) Done.
Waiting for processes to finish.....
Killing processes with signal 9: (init) (aufs) (aufs) (aufs) (aufs)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/0)
A) (khpsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].
```

Așteptați acest mesaj înainte de oprire

34.3. Cum realizez o scanare antivirus?

După ce sistemul a fost pornit, va apărea un program asistent care vă permite să vă scanați complet calculatorul. Trebuie doar să faceți clic pe butonul **Start**.



Notă

Dacă rezoluția ecranului nu este suficient de mare, vi se va cere să porniți scanarea în mod text.

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

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



Notă

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

2. Puteți vedea numărul problemelor care vă afectează sistemul.

Problemele sunt afișate pe grupuri. Faceți clic pe căsuța cu "+" pentru a deschide un grup sau pe căsuța cu "-" pentru a închide un grup.

Puteți alege o acțiune globală care să fie luată asupra fiecărui grup de probleme sau puteți alege acțiuni separate pentru fiecare problemă în parte.

3. Puteți vedea un rezumat al rezultatelor.

Dacă doriți să scanați numai un anumit director, puteți folosi una dintre următoarele variante:

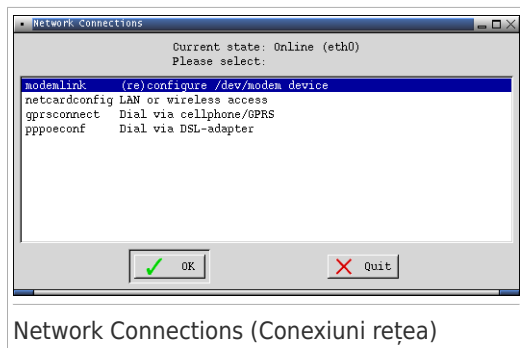
- Folosiți **BitDefender Scanner for Unices**.
 1. Faceți dublu-clic pe iconița START SCANNER de pe desktop. Aceasta va lansa **BitDefender Scanner for Unices**.
 2. Faceți clic pe **Scanner**. Va apărea o nouă fereastră.
 3. Selectați directorul pe care doriți să-l scanați și faceți clic pe **Open** pentru a începe scanarea folosind același asistent care a apărut atunci când ați pornit calculatorul prima dată.
- Folosiți meniul contextual - navigați printre fișiere, faceți clic-dreapta pe fișierul sau pe directorul dorit și selectați **Send to**. Apoi alegeți **BitDefender Scanner**.
- Sau puteți inițializa următoarea comandă de la un terminal. **BitDefender Antivirus Scanner** va începe cu fișierul sau directorul selectat ca locație implicită de scanare.

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

34.4. Cum configurez conexiunea Internet?

Dacă sunteți într-o rețea DHCP și aveți un card de rețea ethernet, conexiunea Internet ar trebui să fie deja detectată și configurată. Pentru configurare manuală, urmați pașii de mai jos.

1. Faceți dublu-clic pe iconița Network Connections (Conexiuni rețea) de pe desktop. Va apărea următoarea fereastră:



2. Selectați tipul conexiunii utilizate și faceți clic pe OK.

Conexiune	Descriere
modemlink	Selectați acest tip de conexiune dacă folosiți un modem și o linie telefonică pentru acces la Internet.

Conexiune	Descriere
netcardconfig	Selectați acest tip de conexiune dacă folosiți o rețea locală (LAN) pentru acces la Internet. A se folosi și pentru conexiuni fără fir (wireless).
gprsconnect	Selectați acest tip de conexiune dacă accesați Internetul prin intermediul unei rețele de telefonie mobilă utilizând protocolul GPRS (General Packet Radio Service). Se poate folosi de asemenea un modem GPRS în locul unui telefon.
pppoeconf	Selectați acest tip de conexiune dacă folosiți un modem DSL (Digital Subscriber Line) pentru acces la Internet.

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



Important

Vă rugăm să țineți cont că prin selectarea opțiunilor de mai sus doar veți activa modemul. Pentru a configura conexiunea de rețea, urmați acești pași:

1. Faceți clic-dreapta pe desktop. Va apărea meniul contextual al BitDefender Rescue CD.
2. Selectați **Terminal (as root)**.
3. Introduceți următoarele comenzi:

```
# pppconfig
```

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

34.5. Cum actualizez BitDefender?

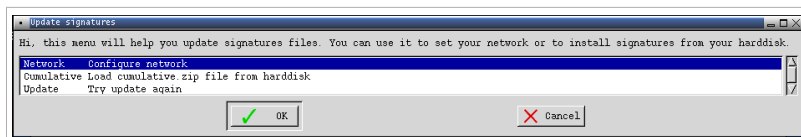
La pornirea sistemului, actualizarea semnăturilor de viruși se face automat. Totuși, dacă ați sărit acest pas sau dacă doriți să actualizați BitDefender după pornirea calculatorului, iată două moduri în care puteți face acest lucru:

● Folosiți **BitDefender Scanner for Unices**.

1. Faceți dublu-clic pe iconița START SCANNER de pe desktop. Aceasta va lansa **BitDefender Scanner for Unices**.
2. Faceți clic pe **Actualizare**.

● Folosiți comanda rapidă **Update Signatures** de pe desktop.

1. Faceți dublu-clic pe iconița Update Signatures de pe desktop. Va apărea următoarea fereastră:



Actualizare semnături

2. Puteți proceda astfel:
 - ▶ Selectați **Cumulative** pentru a instala semnăturile deja salvate pe hard discul dumneavoastră, căutând și încărcând fișierul `cumulative.zip`.
 - ▶ Selectați **Update** pentru a vă conecta imediat la internet și descărca ultimele semnături de viruși.
3. Faceți clic pe **OK**.

34.5.1. Cum actualizez BitDefender printr-un proxy?

Dacă folosiți un server proxy pentru conectarea calculatorului dumneavoastră la Internet, trebuie efectuate anumite configurări pentru a actualiza semnăturile de viruși.

Pentru a actualiza BitDefender printr-un proxy, folosiți una dintre următoarele opțiuni:

- Folosiți **BitDefender Scanner for Unices**.
 1. Faceți dublu-clic pe iconița **START SCANNER** de pe desktop. Aceasta va lansa **BitDefender Scanner for Unices**.
 2. Faceți clic pe **Settings**. Va apărea o nouă fereastră.
 3. Sub **Update Settings**, selectați căsuța **Enable HTTP Proxy**. Specificați gazda Proxy (a se preciza după cum urmează: `gază[:port]`), utilizatorul Proxy (a se preciza după cum urmează: `[domeniu\]utilizator`) și Parola. Selectați căsuța **Ocolire server proxy când nu este disponibil** pentru folosirea unei conexiuni directe dacă serverul proxy nu este disponibil.
 4. Faceți clic pe **Salvează**
 5. Faceți clic pe **Actualizează**
- Folosește Terminalul (ca root).
 1. Faceți clic-dreapta pe desktop. Va apărea meniul contextual al BitDefender Rescue CD.
 2. Selectați **Terminal (as root)**.
 3. Introduceți comanda: `cd /ramdisk/BitDefender-scanner/etc`.
 4. Introduceți comanda: `mcedit bdsfan.conf` pentru a edita acest fișier utilizând GNU Midnight Commander (mc).
 5. Activați următoarea linie: `#HttpProxy =` (prin ștergerea simbolului #) și specificați domeniul, numele de utilizator, parola și portul serverului proxy. De exemplu, linia respectivă poate arăta astfel:

HttpProxy = myuser:mypassword@proxy.company.com:8080

6. Apăsați **F2** pentru a salva fișierul curent, confirmați salvarea și apoi apăsați **F10** pentru a-l închide.

7. Introduceți comanda: **bdsfan update**.

34.6. Cum îmi salvez datele?

Să presupunem că nu puteți porni calculatorul dumneavoastră, cu Windows instalat, din cauza unor probleme necunoscute. În același timp, trebuie neapărat să accesați date importante de pe calculatorul dumneavoastră. Aici este util BitDefender Rescue CD.

Pentru a salva datele dumneavoastră de pe calculator pe un dispozitiv mobil, cum ar fi un stick de memorie USB, urmați acești pași:

1. Introduceți CD-ul cu BitDefender Rescue CD în unitatea CD-ROM, stickul de memorie în USB și apoi reporniți calculatorul.



Notă

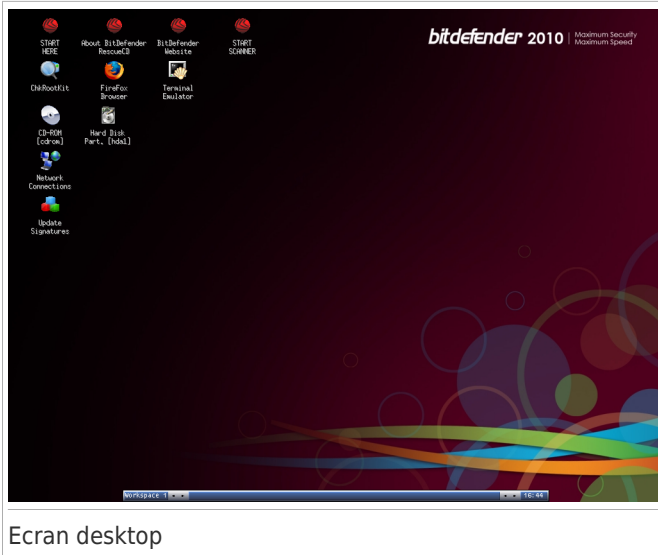
Dacă introduceți stickul de memorie mai târziu, va trebui să montați dispozitivul amovibil urmând acești pași:

- a. Faceți dublu-clic pe iconița Terminal Emulator de pe desktop.
- b. Introduceți următoarea comandă:

```
# mount /media/sdb1
```

Vă rugăm să țineți cont că în funcție de configurația calculatorului dumneavoastră, acesta poate fi `sda1` în loc de `sdb1`.

2. Așteptați până ce BitDefender Rescue CD pornește calculatorul. Va apărea următoarea fereastră:



Ecran desktop

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



Notă

Atunci când lucrați cu BitDefender Rescue CD, veți avea de-a face cu nume de partiții de tip Linux. Așadar, [sda1] va corespunde probabil partiției (C:) din Windows, [sda3] partiției (F:) și [sdb1] stickului de memorie.



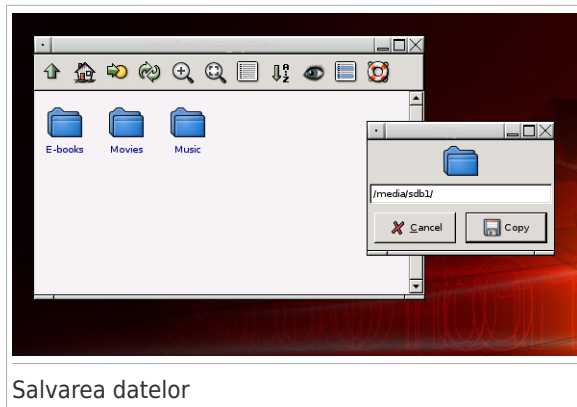
Important

În cazul în care calculatorul nu a fost închis corect, este posibil ca anumite partiții să nu fi fost montate automat. Pentru a monta o partiție, urmați acești pași:

- a. Faceți dublu-clic pe iconița Terminal Emulator de pe desktop.
- b. Introduceți următoarea comandă:

```
# mount /media/partition_name
```

4. Căutați printre directoare și alegeți-l pe cel dorit. De exemplu, MyData care conține subdirectoarele Movies, Music și E-books.
5. Faceți clic-dreapta pe directorul dorit și selectați **Copy**. Va apărea următoarea fereastră.



6. Introduceți `/media/sdb1/` în căsuța de text corespunzătoare și faceți clic pe **Copy**.

Vă rugăm să țineți cont că în funcție de configurația calculatorului dumneavoastră, acesta poate fi `sda1` în loc de `sdb1`.

34.7. Cum folosesc modul consolă?

Dacă rezoluția ecranului dvs nu este destul de mare pentru a rula interfața grafică, puteți lansa BitDefender Rescue CD în modul consolă. Acesta vă permite să efectuați o scanare completă a calculatorului.

Pentru a rula CD-ul în modul consolă, setați BIOS-ul calculatorului dvs să se lanseze de pe CD, introduceți CD-ul în unitate și reporniți calculatorul. Așteptați să apară ecranul de pornire și selectați **Start knoppix in console mode**.

După ce ați pornit sistemul, urmați instrucțiunile de pe ecran pentru a efectua o scanare completă a calculatorului.

BitDefender detectează partițiile de pe hard disc și actualizează automat baza de date cu semnături de viruși, înainte de începutul scanării. BitDefender va dezinfecă toate fișierele infectate identificate. La final, va fi afișat un jurnal cu rezultatele scanării.



Notă

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

Vocabular

ActiveX

ActiveX este un mod de scriere a programelor astfel încât să poată fi apelate de celelalte programe și sisteme de operare. Tehnologia ActiveX este utilizată pentru realizarea de pagini Web interactive care se comportă ca niște aplicații și nu ca niște simple pagini statice. Cu elemente de ActiveX, utilizatorii pot răspunde la întrebări, să utilizeze butoane și să interacționeze și în alte moduri cu pagina Web. Controalele ActiveX sunt adesea scrise utilizând limbajul Visual Basic.

Active X este cunoscut pentru lipsa totală de control al securității; experții în securitatea calculatoarelor descurajează utilizarea lui pe Internet.

Adware

Aplicația adware este adesea combinată cu o aplicație gazdă care este oferită gratuit dacă utilizatorul acceptă aplicația adware. Deoarece aplicațiile adware sunt de obicei instalate după ce utilizatorul a fost de acord în prealabil cu un contract de licențiere care explică scopul aplicației, nu este comisă nicio infracțiune.

Totuși, reclamele de tip pop-up pot fi supărătoare, iar în unele cazuri pot afecta performanțele sistemului. De asemenea, informațiile pe care unele dintre aceste aplicații le adună pot cauza motive de îngrijorare utilizatorilor care nu cunosc în întregime termenii din contractul de licențiere.

Arhivă

Un disc, o casetă sau un director care conține fișiere de rezervă.

Un fișier care conține unul sau mai multe fișiere într-un format comprimat.

Backdoor

Reprezintă o gaură de securitate realizată în mod deliberat. Motivația acestor "găuri" nu este întotdeauna malițioasă: unele sisteme de operare, de exemplu, sunt puse în circulație cu conturi privilegiate pentru tehnicienii din service sau de responsabili cu mentenanță produsului din partea vânzătorului.

Sector de boot

Un sector la începutul fiecărui disc care identifică arhitectura discului (mărimea sectorului, mărimea clusterului și altele). În cazul discurilor de startup, sectorul de boot conține un program care încarcă sistemul de operare.

Virus de boot

Reprezintă un virus care infectează sectorul de boot al unui disc fix sau al unei dischete. Orice încercare de a face boot de pe o dischetă infectată cu un virus de boot va determina virusul să devină activ în memorie. Din acest moment de fiecare dată când veți realiza boot-area sistemului, virusul va deveni activ în memorie.

Browser

Este prescurtarea de la Web Browser, o aplicație utilizată pentru a localiza și încărca pagini de Web. Două din cele mai populare browsere sunt Mozilla Firefox și Microsoft Internet Explorer. Ambele sunt browsere grafice, ceea ce înseamnă că pot afișa atât grafice cât și text. În plus, cele mai moderne browsere pot prezenta informații multimedia, incluzând sunet și animație.

Linie de comandă

Într-o interfață linie de comandă, utilizatorul scrie comenzile în spațiul prevăzut direct pe ecran utilizând limbajul de comandă.

Cookie

Un cookie reprezintă un set de date pe care un server Web îl transmite către un browser atunci când utilizatorul vizitează prima oară site-ul și care este actualizat de fiecare dată când utilizatorul accesează din nou site-ul. Serverul, la fel ca și browserul, salvează informațiile despre utilizator conținute în cookie. Aceste informații sunt stocate sub forma unui fișier text în directoarele de sistem ale browserelor Netscape și Explorer; nu toate browserele suportă cookie. Fișierele cookie stochează informații cum ar fi numele utilizatorului și parola, cât și ce părți din site au fost vizitate. Browserul împarte fiecare cookie doar cu server-ul care l-a generat, celelalte servere le pot citi doar pe cele generate de ele. Unele fișiere cookie sunt programate cu dată de expirare, astfel încât ele vor fi șterse automat după o anumită perioadă de timp.

Drive de disc

Este un dispozitiv care citește date de pe un disc și scrie date pe un disc.

Un drive de hard disc citește / scrie date de pe / pe hard disc.

Un drive de floppy accesează dischetele floppy.

Drive-ele de disc pot fi sau interne (incorporate în interiorul unui calculator) sau externe (plasate într-o locație separată care este conectată la calculator).

Descărcare

Reprezintă copierea (de obicei a unui întreg fișier) de pe o sursă principală pe un dispozitiv periferic. Termenul este adesea utilizat pentru a descrie procesul de copiere a unui fișier de pe un serviciu on-line pe calculatorul unui utilizator. De asemenea se mai poate referi și la copierea unui fișier de pe un server de rețea pe un calculator din rețea.

E-mail

Se referă la poșta electronică. Acesta este un serviciu care transmite mesaje prin intermediul rețelei locale sau globale.

Evenimente

O acțiune sau întâmplare detectată de un program. Evenimentele pot fi acțiuni ale utilizatorului, cum ar fi executarea unui clic cu mouse-ul sau apăsarea unei taste, sau întâmplări în sistem cum ar fi epuizarea memoriei.

Fals pozitiv

Apare atunci când un analizator detectează un fișier ca fiind infectat când de fapt acesta nu este infectat.

Extensie de fișier

Reprezintă porțiunea dintr-un nume de fișier ce urmează după caracterul punct, și care indică tipul de date pe care le stochează fișierul.

Multe sisteme de operare, cum ar fi Unix, VMS, and MS-DOS, utilizează extensii de fișiere. De obicei aceasta este formată din una până la trei caractere (unele sisteme de operare mai vechi nu suportă mai mult de trei). De exemplu: ".txt" pentru fișierele text oarecare, ".c" pentru fișierele sursă scrise în limbajul C, etc.

Metoda euristică

Reprezintă o metodă bazată pe anumite reguli pentru identificarea de viruși noi. Această metodă de scanare nu se bazează pe semnături de viruși cunoscuți. Avantajul metodei euristice e dat de faptul că nu poate fi păcălită de o nouă variantă a unui virus deja existent. Totuși ocazional poate raporta un cod suspicios în programe normale, generând așa-numitul "fals pozitiv".

IP

Internet Protocol - Un protocol rutabil din suita protocoalelor TCP / IP căruia i se atribuie adresarea IP, rutarea, fragmentarea cât și reasamblarea pachetelor IP.

Applet-uri Java

Reprezintă un program Java care este proiectat să ruleze doar pe pagini web. Pentru a utiliza un applet pe o pagină web, trebuie specificate numele applet-ului și mărimea acestuia. Când este accesată o pagină web, browser-ul descarcă applet-ul de pe un server și îl rulează pe mașina utilizatorului (clientul). Applet-urile diferă de aplicații prin aceea că sunt guvernate de un protocol de securitate strict.

Astfel că, deși pot rula pe calculatorul unui utilizator, ele nu pot citi sau scrie date pe aceste calculatoare. Applet-urile sunt restricționate de domeniul de care aparțin în ceea ce privește scrierea și citirea datelor.

Virus de macro

Un tip de virus informatic este acela inclus ca macro într-un document. Multe aplicații cum ar fi de exemplu Microsoft Word și Excel suportă limbaje macro puternice.

Aceste limbaje permit încapsularea de macro-uri în documente și execută aceste macro-uri de fiecare dată când este deschis documentul.

Client de mail

Un client de mail este o aplicație care vă permite să trimiteți și să recepționați mesaje.

Memorie

Reprezintă arii de stocare a datelor din interiorul calculatorului. Termenul de memorie desemnează locul de stocare a datelor pe chipuri și pe cel al cuvintelor pe casete sau cd-uri audio. Fiecare calculator dispune de o anumită capacitate de memorie fizică, referită de obicei prin memorie principală sau RAM.

Metoda ne-euristică

Această metodă de scanare se bazează pe semnături specifice de viruși. Avantajul metodelor ne-euristice constă în aceea că scannerul nu poate fi "păcălit" de ceea ce poate părea un virus și din acest motiv nu generează fals pozitiv.

Programe împachetate

Reprezintă un fișier în format comprimat. Multe din sistemele de operare și aplicații conțin comenzi care vă dau posibilitatea de a împacheta un fișier astfel încât să ocupe mai puțină memorie. De exemplu, să presupunem că aveți un fișier text care conține zece caractere reprezentând spații. În mod normal, acesta ar necesita zece biți de memorie pentru a fi stocați.

Totuși, un program care împachetează fișiere va înlocui caracterele de spațiu printr-un caracter reprezentând spațiu, urmat de un număr care reprezintă numărul de spații care este înlocuit. În acest caz, cele zece caractere reprezentând spațiu ar necesita doar doi biți. Aceasta este doar un exemplu de comprimare - există multe alte metode în afară de aceasta.

Cale

Reprezintă direcția exactă către un fișier de pe un calculator. Această direcție este specificată utilizând sistemul ierarhic de organizare a fișierelor de sus în jos.

Ruta între două puncte, cum ar fi de exemplu canalul de comunicație între două computere.

Phishing

Reprezintă acțiunea de a trimite un e-mail către un utilizator, pretinzând a fi o companie legitimă, în încercarea de a păcăli utilizatorul să furnizeze informații confidențiale ce vor fi folosite la furtul identității. E-mailul îndreaptă utilizatorul către un site Web unde acesta este rugat să actualizeze informații personale, cum ar fi parole și numere de card de credit, de asigurări sociale și de conturi bancare pe care compania respectivă deja le are. Site-ul Web este însă fals și folosit pentru a fura informațiile despre utilizator.

Virus polimorf

Reprezintă un virus care își schimbă forma cu fiecare fișier pe care îl infectează. Din cauză că nu au un tipar binar consistent, asemenea viruși sunt greu de identificat.

Port

Reprezintă o interfață a unui calculator la care se poate conecta un dispozitiv. Calculatoarele personale dispun de diferite tipuri de porturi. Există porturi interne pentru conectarea hard discurilor, monitoarelor și tastaturilor. Există porturi externe pentru conectarea modemului, imprimantei, mouse-ului și a altor dispozitive periferice.

În rețelele TCP / IP și UDP acestea reprezintă un punct terminus al unei conexiuni logice. Numărul portului identifică ce tip de port este. De exemplu, portul 80 este utilizat pentru traficul HTTP.

Fișier de raport

Reprezintă un fișier care listează acțiunile care au avut loc. BitDefender menține un fișier log (jurnal) în care sunt listate obiectele care au fost scanate, numele fișierelor, numărul de arhive și fișiere scanate, câte fișiere infectate și suspecte au fost găsite.

Rootkit

Un rootkit este un set de unelte soft ce oferă acces la nivel de administrator în interiorul unui sistem. Termenul a fost utilizat pentru prima oară pentru sistemele de operare UNIX și se referea la unelte recompilate ce furnizau intrușilor drepturi administrative, permițându-le să își ascundă prezența astfel încât să nu poată fi văzuți de către administratorii de sistem.

Rolul principal al rootkiturilor este de a ascunde procese, fișiere, loginuri și jurnale. Acestea pot de asemenea să intercepteze date de la terminale, conexiuni la rețea sau perifice dacă sunt dotate cu softul adecvat.

Rootkiturile nu sunt malițioase prin natură. De exemplu, sistemele și chiar unele aplicații ascunde fișiere critice utilizând rootkituri. Totuși, ele sunt folosite în general pentru a ascunde aplicații malițioase sau prezența intrușilor în sistem. În combinație cu aplicații malițioase, rootkiturile constituie o mare amenințare pentru securitatea și integritatea sistemului. Acestea pot monitoriza traficul, crea porți de acces în sistem ("backdoors"), altera fișiere și jurnale și evita detecția.

Script

Un alt termen pentru fișiere macro sau de tip "bat", un script reprezintă o listă de comenzi care pot fi executate fără intervenția utilizatorului.

Spam

Termen ce acoperă întregă gamă a mesajelor electronice nesolicitate.

Spyware

Reprezintă orice software care strânge informații despre utilizator prin intermediul conexiunii la Internet fără știrea acestuia, de obicei în scopuri publicitare. Aplicațiile spyware sunt de obicei primite ca parte ascunsă a unui program de tip freeware sau shareware, ce poate fi descărcat de pe Internet; totuși, trebuie știut că majoritatea aplicațiilor de tip shareware și freeware nu

conțin aplicații spyware. Odată instalată, aplicația spyware monitorizează activitatea utilizatorului pe Internet și transmite pe ascuns informații altei persoane. Aplicațiile spyware pot aduna, de asemenea, informații despre adresele e-mail și chiar parole și numere de carduri de credit.

Asemănarea dintre spyware și un cal troian este faptul că utilizatorul instalează aplicația fără voia sa atunci când instalează altceva. Un mod obișnuit de a deveni victimă unei aplicații spyware este de a descărca prin rețelele peer-to-peer anumite produse de schimb de fișiere care sunt disponibile astăzi.

Pe lângă problemele legate de etică și intimitate, aplicația spyware fură de la utilizator atât prin folosirea memoriei calculatorului cât și a lungimii de bandă deoarece trimite informații înapoi la sursă prin intermediul conexiunii la Internet a utilizatorului. Deoarece folosesc memorie și resurse ale sistemului, aplicațiile spyware pot conduce la blocarea sistemului sau la instabilitate generală.

Elemente din startup

Orice fișier plasat în acest director se va deschide de fiecare dată când calculatorul este pornit. De exemplu, un sunet care se va auzi atunci când este pornit calculatorul sau chiar aplicații sunt considerate elemente de startup. În mod normal, un alias al programului este plasat în acest director, și nu direct fișierul.

Bara de sistem

Introdusă odată cu apariția sistemului Windows 95, bara de sistem este plasată în taskbar-ul de Windows (situat lângă ceas) și conține iconițe pentru accesul rapid la aplicații sistem cum ar fi cele legate de fax, imprimantă, modem, volum, și altele. Executați dublu-clic cu mouse-ul pe o iconiță pentru a vizualiza și accesa elementele.

TCP/IP

Transmission Control Protocol/Internet Protocol - Un set de protocoale de rețea folosite în mod larg în domeniul Internet și care asigură comunicarea între rețelele de calculatoare interconectate având arhitecturi hardware și sisteme de operare diferite. TCP/IP include standarde referitoare la realizarea comunicării între calculatoare cât și convenții folosite în conectarea rețelelor și rutării traficului.

Troian

Este un program distructiv care este mascat sub forma unei aplicații benigne. Spre deosebire de viruși, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cei mai mascați troieni este acela care pretinde că elimină virușii de pe computerul dumneavoastră, dar în loc de aceasta, introduce viruși pe calculatorul dumneavoastră.

Termenul provine de la o poveste din opera "Iliada" lui Homer, în care grecii oferă dușmanilor lor, troienii, în semn de pace un cal gigantic de lemn. Dar după ce troienii aduc acest cal în interiorul orașului lor, din interiorul calului ies

o mulțime de soldați greci, care deschid porțile cetății, permițându-le celorlalți soldați greci să pătrundă în oraș și să captureze Troia.

Actualizare

O versiune nouă de produs hardware sau software proiectat să înlocuiască o versiune mai veche a aceluiași produs. În afară de acesta, rutinele de instalare verifică dacă există instalată pe calculatorul dumneavoastră o altă versiune mai veche; dacă nu, nu puteți instala actualizarea.

BitDefender dispune de modulul său propriu care realizează actualizarea automată sau manuală.

Virus

Reprezintă un program sau o bucată de cod care se încarcă pe calculator fără știrea dumneavoastră și rulează independent de voința dumneavoastră. Cea mai mare parte a virușilor se pot și înmulți. Toți virușii informatici sunt creați de om. Un simplu virus care poate realiza copii ale sale este relativ simplu de produs. Chiar și un asemenea virus este periculos întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. Un virus și mai periculos este acela care este capabil să se răspândească în rețea și poate să treacă de sistemele de securitate.

Semnătură de virus

Reprezintă tiparul binar al unui virus, utilizat de un program antivirus pentru detecția și eliminarea virusului.

Vierme

Reprezintă un program care se autopropagă în interiorul unei rețele, reproducându-se pe măsură ce se răspândește. Nu se poate atașa la alte programe.