BitDefender 8 Standard

Manual de utilizare

bitdefender
secure your every bit

Cuprins

Contract de licențiere 4

Licență software **4**

Licența şi garanția produsului **5**

BitDefender Rescue System 7

Cerințe de sistem **7**

Mod de scanare **7**

Porniți calculatorul cu ajutorul CD-ului 7

Instalați driver-ul NTFS 8

Verificați hard discul 8

Selectați opțiunile de scanare 8

Porniți procesul de scanare 10

Instalarea 11

Cerințe de sistem **11**

Etapele de instalare **11**

Dezinstalarea, repararea sau modificarea componentelor instalate **13**

Descriere şi caracteristici 14

Descriere **14**

Caracteristici **14**

Antivirus 14

Actualizare 15

Alte caracteristici **15**

Consola de administrare 16

Privire generală **16**

Modulul General **18**

Status 18

Înregistrare produs 20

Setările consolei de administrare 21
Info 22
Modulul Antivirus 23
Scanarea la acces 24
Control Regiştri 24
Faceți cele mai importante setări 26
Alte opțiuni 26
Scanarea la cerere 28
Scanare imediată 28
Scanarea programată 36
Izolarea fişierelor infectate 44
Vizualizarea fişierelor de raport 46
Eliminarea viruşilor 47
Modulul Actualizare 48
Actualizare manuală 49
Actualizare automată 50
Locația de actualizare 50
Actualizare automată 51
Opțiuni interfață 51

Recomandări de utilizare 52
Antivirus 52

Întrebări frecvente 53
General 53
Antivirus 53
Actualizare 54

Vocabular 55

Informații de contact 59

1

Contract de licențiere

Licență software

Pachetul BitDefender este protejat de legile de copyright şi de tratatele internaționale privind proprietatea intelectuală. Legea copyright-ului, la fel ca orice alte legi ce privesc proprietatea intelectuală, protejează în multe țări drepturile proprietarului asupra software-ului, acordându-i câteva drepturi exclusive, cum ar fi dreptul de a copia şi reproduce software-ul.

Copierea software-ului fără permisiunea proprietarului reprezintă încălcarea copyright-ului şi se pedepseşte conform legilor în vigoare.

Se consideră că software-ul este copiat atunci când:

- Se încarcă software-ul în memoria calculatorului de pe o dischetă, de pe hard disc, de pe CD-ROM sau pe altă cale;
- Se copiază software-ul pe un alt suport, cum ar fi o dischetă, CD sau hard disc;
- Lansarea în execuție de pe un server de rețea unde este stocat sau rezident soft-ul respectiv.

Aproape orice software comercial este licențiat în mod direct sau indirect deținătorului de copyright - dezvoltatorul de software - pentru utilizarea finală prin aşa numitul “Contract de licențiere”.

Produsele software pot avea tipuri diferite de contracte de licențiere. BitDefender şi logo-urile BitDefender sunt mărci înregistrare aparținând SOFTWIN.

Licența şi garanția produsului

DACĂ NU SUNTEȚI DE ACORD CU CONDIȚIILE ŞI TERMENII PRECIZAȚI AICI, VĂ RUGĂM SĂ NU INSTALAȚI ACEST PRODUS. APĂSÂND pe unul dintre următoarele butoane “ACCEPT”, “DA”, “CONTINUA”, INSTALÂND sau UTILIZÂND acest software ÎN ORICE MOD, INDICAȚI CĂ ÎNȚELEGEȚI PERFECT TERMENII ACESTUI CONTRACT DE LICENȚIERE ŞI ÎI ACCEPTAȚI ÎN TOTALITATE.

Acest Contract de Licențiere reprezintă o înțelegere legală între dumneavoastră (ca persoană fizică sau juridică) şi SOFTWIN pentru utilizarea produsului software identificat aici ca “BitDefender”, aparținând SOFTWIN, care include atât software-ul cât şi suportul fizic asociat, materialele tipărite, documentația “on line” şi cea electronică. Toate acestea sunt protejate de legislația internă şi internațională privind drepturile de autor şi proprietatea intelectuală. Prin instalarea, copierea sau orice alt tip de utilizare a produsului BitDefender, acceptați termenii acestui contract. Dacă nu sunteți de acord cu termenii acestui contract, nu instalați şi nu utilizați produsul BitDefender. Puteți returna produsul la vânzător pentru returnarea banilor în maxim 30 de zile de la cumpărare. Pentru aceasta, vi se va solicita dovada achiziționării produsului.

BitDefender este protejat de tratatele şi legile internaționale privind proprietatea intelectuală, cât şi de celelalte legi şi tratate privind drepturile de autor. BitDefender este licențiat şi nu vândut.

ACORDAREA LICENȚEI. SOFTWIN vă oferă următoarele condiții de licențiere pentru BitDefender:

APLICAȚIA SOFTWARE. O licență de utilizare vă dă dreptul de a instala şi a utiliza o copie a produsului BitDefender pe un singur terminal. Pentru a utiliza BitDefender pe mai multe stații de lucru se aplică regulile pachetului de licențe descris in secțiunea UTILIZAREA ÎN REȚEA.

UTILIZAREA ÎN REȚEA. Puteți stoca sau instala o copie a produsului BitDefender pe un terminal de stocare, cum ar fi un server de rețea, utilizat numai pentru instalarea sau rularea sa pe celelalte computere din rețeaua internă; în orice caz, va trebui să cumpărați şi să dedicați câte o licență separată pentru fiecare calculator din rețea pe care este instalat sau rulează BitDefender de pe server. O singură licență BitDefender nu poate fi împărțită sau utilizată în mod concurent pe mai multe calculatoare. Va trebui să achiziționați un pachet de licențe, dacă doriți licențe multiple pentru instalarea şi utilizarea produsului BitDefender pe mai multe calculatoare. Numărul de terminale pe care este instalată şi utilizată aplicația trebuie să fie egal sau mai mic decât numărul de licențe acordate.

PACHETUL DE LICENȚE. Dacă achiziționați Pachetul de Licențe şi ați obținut şi Contractul de Licențiere pentru licențe multiple de utilizare BitDefender, puteți face un număr de copii adiționale pentru partea software a produsului BitDefender specificat mai sus sub denumirea de “Copii licențiate”.

TERMENI DE LICENȚIERE. Licența acordată începe la data la care veți instala, copia sau utiliza în orice alt mod, pentru prima dată, produsul BitDefender, şi va continua doar pentru calculatorul pe care ați instalat inițial produsul.

ACTUALIZĂRI DE PRODUS (UPGRADE-URI). Dacă BitDefender este etichetat ca upgrade, pentru a putea utiliza BitDefender va trebui să dețineți licență de utilizare a unui produs identificat de SOFTWIN ca fiind eligibil pentru un upgrade. Un produs BitDefender etichetat ca fiind upgrade, înlocuieşte sau completează produsul care reprezintă baza pentru eligibilitatea efectuării de upgrade. Puteți utiliza produsul rezultat în urma upgrade-ului numai în concordantă cu termenii specificați în prezentul Contract de Licențiere. Dacă BitDefender este un upgrade al unei componente a pachetului de programe software care au fost licențiate ca un singur produs, atunci BitDefender poate fi utilizat sau transferat numai ca parte a acelui

singur pachet de produse şi nu poate fi separat pentru utilizarea sa pe mai mult de un singur calculator.

COPYRIGHT. Toate drepturile, titlul şi toate profiturile asupra şi de la BitDefender cât şi drepturile de copiere pentru BitDefender (incluzând, dar nu limitându-se la orice imagine, fotografie, animaţie, video, audio, muzică, text şi cod încorporate în produsul BitDefender), toate materialele tipărite ce însoţesc produsul şi orice copie a produsului BitDefender sunt proprietatea SOFTWIN. BitDefender este protejat de legile şi tratatele internaţionale privind drepturile de autor şi proprietatea intelectuală. Din acest motiv trebuie să trataţi BitDefender ca pe orice alt material cu drepturi de copyright. Aveţi dreptul de a instala BitDefender pe un singur calculator şi puteţi face o singură copie a acestuia doar în scop de siguranţă sau de arhivare a acestuia. Nu puteţi face copii ale documentelor tipărite ce însoţesc produsul BitDefender. Sunteţi obligat să includeţi toate documentele de copyright în forma lor originală pentru toate copiile create, indiferent de mediul de transmisie sau de forma în care BitDefender există. Este interzisă sub-licenţierea, închirierea, vânzarea sau leasing-ul produsului BitDefender. De asemenea, este interzisă piratarea, recompilarea, dezasamblarea, crearea de produse derivate, modificarea, traducerea sau orice altă încercare de a descoperi codul sursă al produsului BitDefender.

LIMITAREA GARANŢIEI. SOFTWIN garantează că suportul de distribuire al produsului BitDefender nu conţine defecte, pentru o perioada de 30 de zile de la data achiziţionării de către dumneavoastră a produsului BitDefender. Singurul remediu în cazul unui defect al suportului de distribuire este înlocuirea de către SOFTWIN a suportului pentru produs pe baza chitanţei de achiziţie, după returnarea suportului defect, sau returnarea banilor pe care i-aţi plătit pentru produsul BitDefender. SOFTWIN nu garantează continuitatea produsului, lipsa erorilor sau că acele erori vor fi corectate. SOFTWIN nu garantează că BitDefender va satisface cerinţele dumneavoastră.

PRIN ACEASTA SOFTWIN NU REVENDICĂ NICI O ALTĂ GARANŢIE PENTRU BitDefender, SPECIFICATĂ SAU IMPLICITĂ. ACEASTĂ LICENŢĂ ESTE EXCLUSIVĂ ŞI ÎNLOCUIEŞTE ORICE ALTĂ GARANŢIE, SPECIFICATĂ SAU IMPLICITĂ, INCLUZÂND GARANŢIA IMPLICITĂ DE COMERCIALIZARE SAU UTILIZARE PENTRU UN SCOP PARTICULAR. ACEASTĂ GARANŢIE VĂ OFERĂ DREPTURI LEGALE SPECIFICE.

TERMENI LEGALI. Oricine utilizează, testează sau evaluează BitDefender va suporta toate riscurile ce derivă din utilizarea BitDefender. În nici un caz, SOFTWIN nu va fi răspunzător pentru nici un tip de stricăciune, incluzând, fără limitare, stricăciunile directe sau indirecte ce reies din utilizarea, rularea sau furnizarea produsului BitDefender, chiar dacă SOFTWIN a fost prevenit de existenţa sau posibilitatea apariţiei unor asemenea stricăciuni. Condiţiile prevăzute în această secţiune se vor aplica indiferent dacă utilizaţi, evaluaţi sau testaţi BitDefender.

ANUNŢ IMPORTANT PENTRU UTILIZATORI: ACEST SOFTWARE POATE CONŢINE ERORI ŞI NU ESTE PROIECTAT PENTRU UTILIZAREA ÎNTR-UN MEDIU CARE IMPLICĂ UN GRAD MARE DE RISC ŞI CARE NECESITĂ PERFORMANŢE RIDICATE. ACEST PRODUS SOFTWARE NU ESTE DESTINAT UTILIZĂRII ÎN OPERAŢII DIN DOMENIUL AVIAŢIEI, DIN SECTORUL NUCLEAR, SAU ÎN SISTEMUL DE COMUNICAŢII, ÎN SECTORUL ARMAMENTULUI, ÎN SISTEMELE CE PRIVESC ÎNTREŢINEREA DIRECTĂ SAU INDIRECTĂ A VIEŢII, CONTROLUL TRAFICULUI AERIAN, SAU ORICE ALTĂ APLICAŢIE SAU INSTALAŢIE ÎN CARE O EROARE AR PUTEA AVEA CA REZULTAT MOARTEA, RANIRI FIZICE SEVERE SAU DAUNE ÎMPOTRIVA PROPRIETĂŢII.

Preţurile, costurile şi tarifele pentru BitDefender pot fi subiectul unor modificări despre care puteţi să nu fiţi înştiinţat. În eventualitatea unei invalidităţi a oricărei clauze din prezentul Contract de Licenţiere, invaliditatea nu va afecta celelalte părţi componente ale prezentului contract. BitDefender şi logo-urile BitDefender sunt mărci înregistrate ale SOFTWIN.

2

BitDefender Rescue System

BitDefender 8 Standard se găseşte pe un CD boot-abil împreună cu **BitDefender Rescue System,** bazat pe **LinuxDefender**, capabil să scaneze şi să dezinfecteze toate mediile de stocare hard înainte de pornirea sistemului de operare.

Folosiți **BitDefender Rescue System** atunci când sistemul dumneavoastră de operare nu mai funcționează corect din cauza infecției cu viruşi. De obicei, acest lucru se întâmplă atunci când nu folosiți un program antivirus.

Actualizarea semnăturilor de viruşi se face automat, fără ca utilizatorul să intervină, de fiecare dată când **BitDefender Rescue System** porneşte.

Cerințe de sistem

- Procesor: Minimum Pentium 2/300MHz sau superior;
- Memorie RAM: 64 MB pentru mod text, cel puțin 256 MB pentru interfață grafică KDE (512 MB recomandat);
- Placă video: Standard compatibilă SVGA.

Mod de scanare

Paşi de urmat pentru scanarea calculatorului împotriva viruşilor.

Porniți calculatorul cu ajutorul CD-ului

Introduceți CD-ul BitDefender în CD-ROM şi reporniți calculatorul.

Această operație va lansa automat **BitDefender Rescue System** (este posibil să fie necesar să setați din BIOS pornirea calculatorului dumneavoastră de pe CD; veți găsi informații despre această operație în “Manualul de Utilizare” a plăcii de bază a calculatorului).

Interfața grafică **BitDefender Rescue System** va apărea:

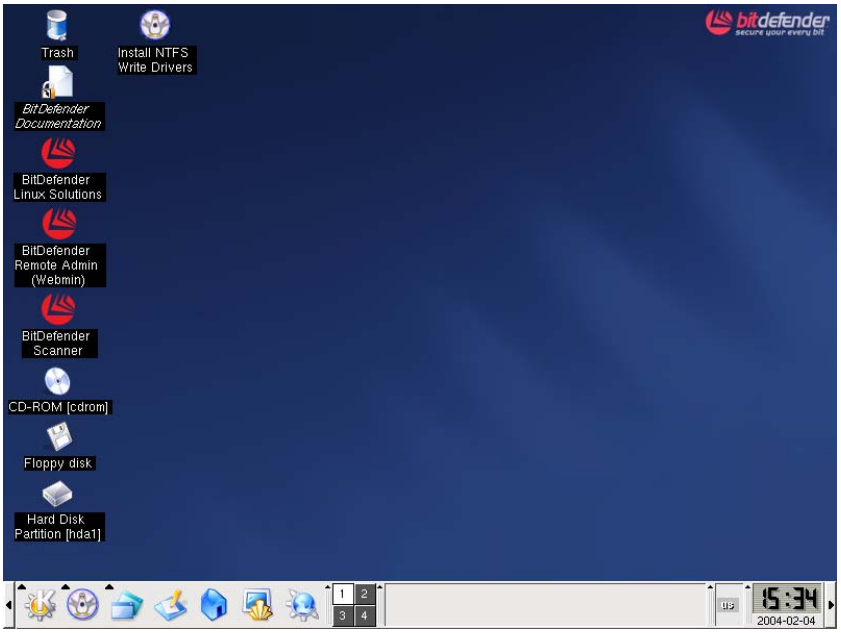


Figura 1

Instalați driver-ul NTFS

Faceți clic pe icoana **Install NTFS Write Drivers** cu butonul din stânga de la mouse. În fereastra care va apărea faceți dublu-clic pe **Forward**. Aceasta va porni instalarea driver-ului NTFS. **LinuxDefender** necesită două drivere (`ntoskrnl.exe` şi `ntfs.sys`) pentru a avea acces la hard disc. În mod curent, doar drivere de Windows XP sunt suportate. A se reține că puteți să le folosiți şi pentru accesarea partițiilor de Windows 2000/NT/2003.

În timpul procesului de instalare veți primi următorul mesaj:
`Cannot open target file "/var/lib/capative/ext2fsd.sys": Read-only file System`.

Confirmați cu **OK**. La final faceți clic pe **OK** pentru a închide procesul de instalare.

Veți primi următorul mesaj: `Although essential modules ...`. Faceți clic pe **OK**.

Verificați hard discul

În interfața **LinuxDefender** faceți clic pe icoana **Hard Disk Partition [hda1]**. Astfel veți deschide o fereastră în care veți vedea conținutul hard discului. Închideți această fereastră.

Selectați opțiunile de scanare

Faceți clic pe icoana **BitDefender Scanner** pentru a selecta opțiunile de scanare. Fereastra următoare va apărea:

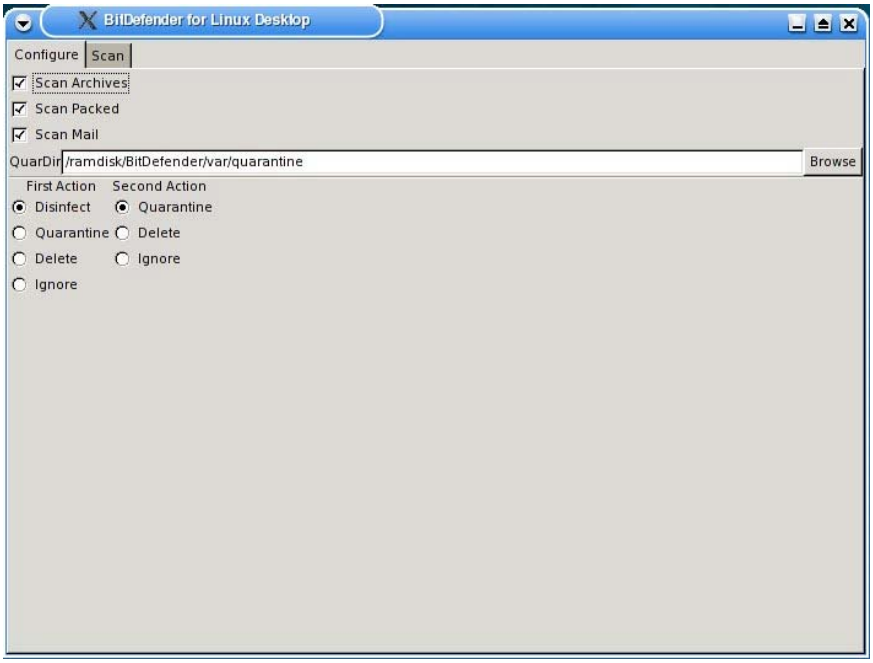


Figura 2

Opțiunile următoare sunt disponibile:

- **Scan Archives** - Scanează în interiorul arhivelor.
- **Scan Packed** – Scanează programele împachetate.
- **Scan Mail** – Scanează mesajele electronice.
- **QuarDir** – Calea implicită la directorul de carantină este: `/ramdisk/BitDefender/var/quarantine`. Dacă doriți să schimbați directorul de carantină faceți clic pe **Browse** şi selectați o altă locație (sau puteți introduce calea în câmpul **QuarDir**).

BitDefender va încerca realizarea unei acțiuni la descoperirea unui fişier infectat. Puteți selecta ce acțiune va fi rulată. Dacă din diferite motive prima acțiune nu poate fi realizată, o a doua acțiune (tot configurabilă) va fi realizată.

SFAT: Recomandăm folosirea **Disinfect** ca primă acțiune şi **Delete** pentru cea de-a doua acțiune.

Puteți selecta acțiunile:

Prima acțiune	Descriere
Disinfect	Pentru dezinfecția fişierului infectat.
Quarantine	Fişierele infectate sunt mutate în carantină. Când părăsiți **BitDefender Rescue System**, directorul de carantină va fi şters.
Delete	Şterge fişierele infectate imediat, fără nici o avertizare.
Ignore	Dacă un fişier infectat va fi detectat, acesta va fi ignorat.

A doua acțiune	Descriere
Quarantine	Fişierele infectate sunt mutate în carantină. Când părăsiți **BitDefender Rescue System**, directorul de carantină va fi şters.
Delete	Şterge fişierele infectate imediat, fără nici o avertizare.
Ignore	Dacă un fişier infectat va fi detectat, acesta va fi ignorat.

Porniți procesul de scanare

Faceți clic pe tab-ul **Scan**.

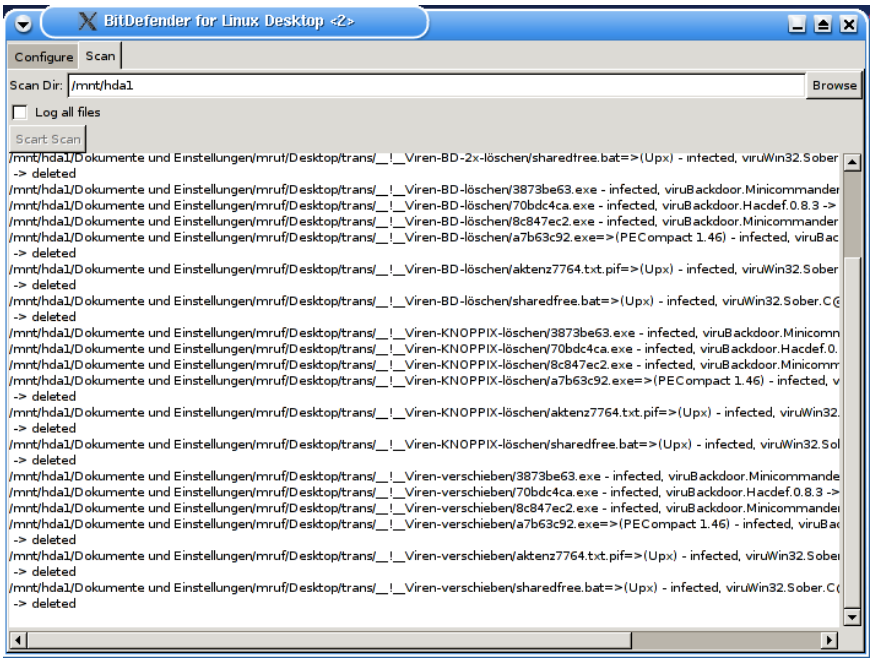


Figura 3

În câmpul **Scan Dir** trebuie să specificați calea la hard disc după cum puteți vedea în exemplul următor.

Exemple:

Dacă aveți un hard disc cu 3 partiții, trebuie să scanați fiecare partiție separat.

- `/mnt/hda1` – pentru prima partiție;
- `/mnt/hda2` – pentru a doua partiție;
- `/mnt/hda3` – pentru a treia partiție.

Dacă aveți şi alt hard disc cu două partiții sintaxa este:

- `/mnt/hdb1`– pentru prima partiție;
- `/mnt/hdb2`– pentru a doua partiție.

Dacă folosiți un hard disc SCSI cu două partiții sintaxa este:

- `/mnt/sda1`– pentru prima partiție;
- `/mnt/sda2`– pentru a doua partiție.

Prin setările implicite opțiunea **Log all files** este dezactivată pentru că viteza de scanare este vizibil mai mică cu această opțiune activată.

Faceți clic pe **Start Scan**. Aceasta va porni procesul de scanare.

Când un virus este găsit, BitDefender vă va informa în fereastra principală.

Notă

Vă recomandăm să scanați de două ori. Este posibil ca virusul să nu fi putut fi şters la prima scanare a unei partiții NTFS.

3

Instalarea

Cerințe de sistem

Pentru funcționarea corespunzătoare a produsului, înainte de instalare, verificați dacă sunt îndeplinite următoarele cerințe de sistem:

Procesor: minimum Pentium 200MHz;
Spațiu pe disc: minimum 40 MB;
Memorie RAM: minimum 64 MB (128 MB recomandat);
Sistem de operare: Windows 98/NT-SP6/Me/2000/XP; IE 4.0 (sau superior).

Etapele de instalare

Faceți dublu-clic pe fişierul de instalare. Imediat veți fi întrebat in ce limba doriți sa rulați produsul:

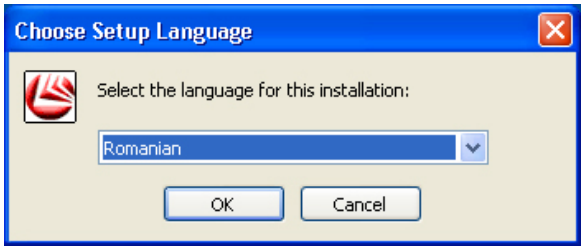


Figura 4

Selectați **Romanian** si faceți clic pe **OK**.

Va apărea fereastra de întâmpinare a programului asistent care vă va conduce prin toate etapele procesului de instalare.

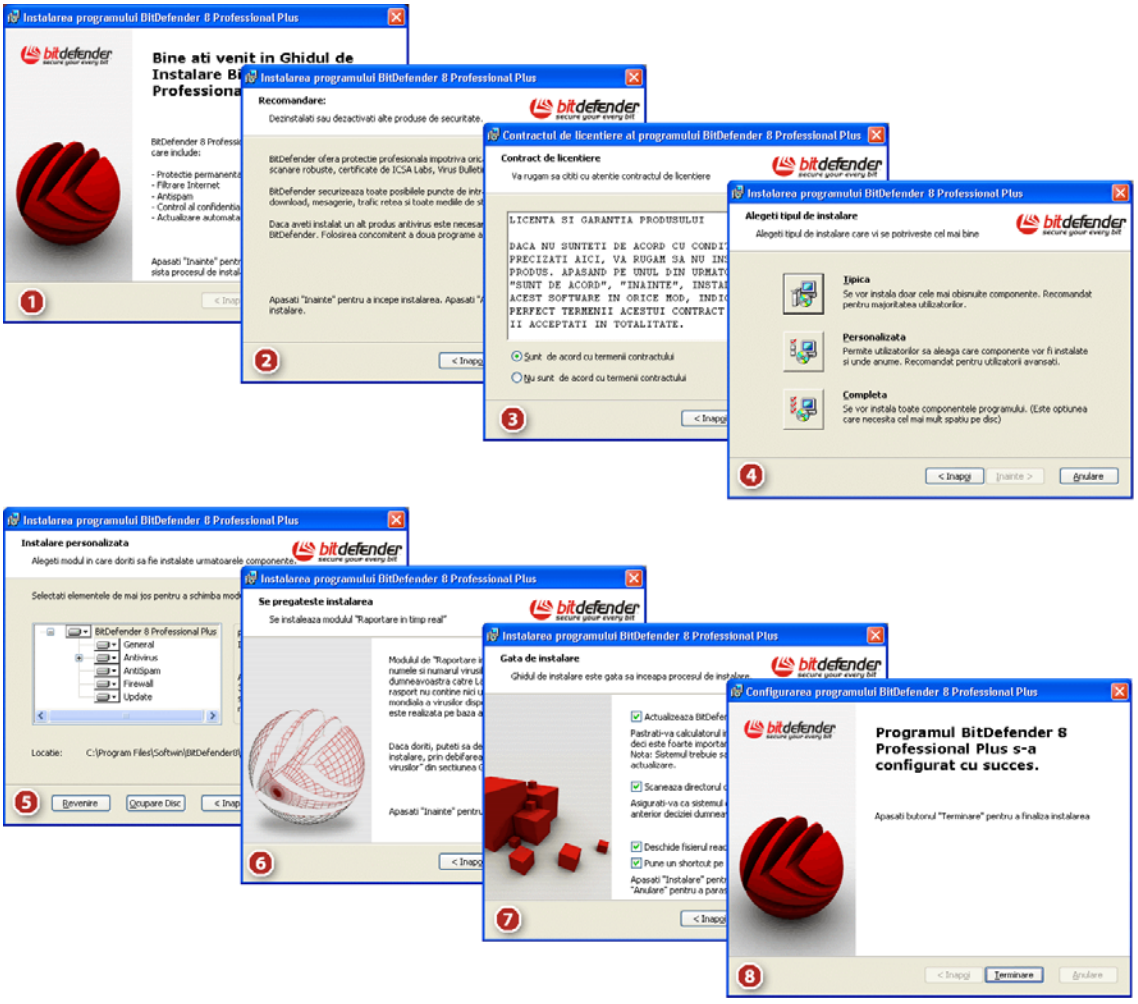


Figura 5

Paşii de instalare:

1. Apăsaţi **Inainte** pentru a continua sau apăsaţi **Anulare** dacă doriţi să părăsiţi procesul de instalare.
2. Apăsaţi **Inainte** pentru a continua sau apăsaţi **Inapoi** pentru a reveni la primul pas.
3. Vă rugam să citiţi cu atenţie **Contractul de Licenţiere** pentru utilizatorul final. Dacă sunteţi de acord cu condiţiile prevăzute aici, selectaţi **Sunt de acord cu termenii contractului** şi apăsaţi **Inainte**. Dacă nu sunteţi de acord cu prevederile acestui contract, selectaţi **Nu sunt de acord cu termenii contractului**, fapt care va determina ieşirea din procesul de instalare.
4. Puteţi alege ce tip de instalare doriţi: tipica, personalizata sau completa.

   - **Tipica** – pentru instalarea celor mai folosite module BitDefender. Recomandată pentru majoritatea utilizatorilor.
   - **Personalizata** – Pentru instalarea personalizată a produsului, permiţând instalarea componentelor dorite de dumneavoastră precum şi alegerea locaţiei de instalare. Este recomandată în special utilizatorilor avansaţi.
   - **Completa** – Pentru instalarea completă. Toate modulele BitDefender vor fi instalate.

   Dacă selectaţi instalarea **Tipica** sau **Completa** veţi sări peste pasul 5.

5. Dacă selectaţi opţiunea **Personalizata** va apărea o nouă fereastră în care vor fi listate toate componentele BitDefender şi din care le puteţi selecta pe cele dorite.

Dacă faceţi clic pe oricare din componente, în partea dreaptă va apărea o scurtă descriere a modulului şi spaţiul necesar pe hard disc pentru instalarea acestuia. De asemenea dacă faceţi clic pe oricare din butoanele  vă va apărea o fereastră în care puteţi alege să instalaţi sau nu modulul selectat.

Puteți alege calea unde doriți să instalați produsul. Directorul setat implicit este `C:\Program Files\Softwin\BitDefender 8`.

Dacă doriți să instalați în alt director, faceți clic pe butonul **Cauta** şi selectați o altă cale.

6. Faceți clic pe butonul **Inainte** pentru a trece la pasul următor.
7. Există patru opțiuni selectate implicit:
   - ➔ **Actualizeaza BitDefender** – Pentru actualizarea BitDefender la sfârşitul instalării. Procesul de actualizare necesită conexiune Internet.
   - ➔ **Ruleaza o scanare completa a sistemului** – Pentru o scanare completă a calculatorului la sfârşitul instalării.
   - ➔ **Deschide fisierul readme** – Pentru deschiderea fişierului readme la sfârşitul instalării.
   - ➔ **Plaseaza un shortcut pe desktop** – Pentru a crea o scurtătură (shortcut) pe desktop la finalizarea instalării.

   Apăsați **Instalare** pentru a lansa instalarea programului.
8. Apăsați **Terminare** pentru a încheia instalarea produsului. După instalare, dacă ați acceptat setările de cale implicite, veți observa că în directorul **Program files** apare subdirectorul **Softwin**, conținând un alt subdirector, **BitDefender 8**.

Notă
Este posibil ca la finalul instalării sa fiți întrebat dacă doriți să reporniți sistemul. Vă recomandăm să faceți asta cât mai curând.

Dezinstalarea, repararea sau modificarea componentelor instalate

Dacă doriți să modificați sau să dezinstalați componentele instalate inițial, selectați **Start** → **Programs** → **BitDefender** → **Modificare, Reparare sau Dezinstalare** din meniul Windows.

Veți fi solicitat să confirmați alegerea dumneavoastră apăsând **Inainte**. Din fereastra ce apare selectați opțiunea dorită:

- **Modificare** – Pentru instalarea de noi componente sau dezinstalarea altora instalate anterior.
- **Reparare** – Pentru reinstalarea tuturor componentelor programului.
- **Dezinstalare** – Pentru dezinstalarea produsului şi a tuturor componentelor sale.

Pentru a continua procesul de instalare, va trebui să selectați una din aceste trei opțiuni. În cazul în care doriți să instalați o nouă versiune vă sugerăm să alegeți întâi opțiunea **Dezinstalare** pentru eliminarea componentelor anterior instalate şi abia apoi să instalați noua versiune. Va apărea o nouă fereastră de unde puteți selecta opțiunea **Trimite feedback** pentru a ne transmite motivele dezinstalării programului **BitDefender 8**. După finalizarea procesului de dezinstalare vă recomandăm să ştergeți subdirectorul **Softwin** din directorul **Program Files**.

4

Descriere şi caracteristici

Descriere

Din păcate, într-o rețea de calculatoare, un program antivirus bun nu este de ajuns. Amenințările la adresa calculatoarelor şi rețelelor nu vin numai de la viruşi, ci şi de la persoane rău intenționate. Echipa BitDefender este conştientă de amenințările ce pot apărea într-un mediu informatizat şi de aceea a conceput un pachet complet, destinat securității datelor.

BitDefender 8 Standard integrează modulele **Antivirus** şi **Actualizare** într-un pachet de securitate cuprinzător, adaptat atât nevoilor utilizatorilor individuali, cât şi marilor corporații din întreaga lume.

Caracteristici

BitDefender 8 Standard include 2 module de protecție: **Antivirus** şi **Actualizare**.

Antivirus

Misiunea modulului Antivirus este aceea de a detecta şi îndepărta toți viruşii care amenință securitatea datelor dumneavoastră. BitDefender Antivirus utilizează motoare de scanare puternice, certificate de **ICSA Labs**, **Virus Bulletin, Checkmark, Checkvir** şi **TUV**.

Protecție Antivirus permanentă

Noile motoare de scanare BitDefender sunt îmbunătățite şi vor scana şi dezinfecta fişierele infectate la accesarea lor de către utilizator, minimizând pierderile de date. Documentele infectate pot fi acum recuperate, în loc să fie şterse.

Protecția aplicațiilor Peer-2-Peer

BitDefender detectează viruşii care se transmit prin intermediul aplicațiilor de mesagerie şi transfer de fişiere.

Analiză comportamentală

Blochează aplicațiile malițioase în baza unei analize comportamentale. Această metodă asigură protecție activă împotriva viruşilor noi, Troieni, viermi Internet şi potențiale coduri virale. Fişierele de sistem, regiştrii şi activitatea Internet sunt monitorizate în mod constant.

Carantină
Fişierele infectate sau suspecte pot fi copiate pentru siguranță, într-o zonă sigură de carantină înainte de a fi dezinfectate sau şterse. Conținutul carantinei poate fi trimis la Laboratorul BitDefender pentru analiză detaliată. Fişierele care s-au dovedit inofensive pot fi restaurate cu uşurință la pozițiile lor anterioare.

Protecție completă e-mail
Aplicația rulează la nivelul protocolului POP3, blocând orice mesaj infectat, indiferent de clientul de e-mail utilizat (MS Exchange, MS Outlook, MS Outlook Express, Netscape, Eudora, Lotus Notes, Pegasus, The Bat, etc.), fără altă configurare adițională.

Actualizare

Acesta este modulul prin care se face actualizarea produsului, cu noi semnături de viruşi şi noi caracteristici.

Actualizări rapide şi gratuite
Actualizări inteligente ale protecției antivirus, fără intervenția utilizatorului. Actualizarea poate fi realizată din rețea, de pe Internet, direct sau printr-un server Proxy. Proprietarii de licență BitDefender beneficiază de actualizare gratuită a definițiilor de viruşi şi a produsului.

Auto-reparare
Produsul este capabil să se repare singur dacă este necesar, prin descărcarea fişierelelor lipsă sau afectate, de pe serverele BitDefender.

Actualizare automată
Actualizările pentru motoarele Antivirus sunt gratuite şi complet automate. Căutările de actualizări pot fi programate oricât de des este necesar.

Alte caracteristici

Informație pentru decizii
Programele asistente vă vor ghida prin toate procedurile ce sunt necesare pentru securizarea sistemului. O bază de date uşor de folosit, “trusted apps”, conține informații din care puteți afla dacă aplicațiile care cer acces la rețea sunt de încredere, putând astfel să luați decizii corecte.

Uşor de instalat şi de folosit
O interfață prietenoasă face instalarea şi utilizarea produsului mai uşoară pentru dumneavoastră. Bara de scanare Fişiere vă permite să folosiți drag & drop pentru a scana fişierele mult mai uşor.

Suport tehnic profesional 24/7
Oferit de reprezentanți calificați şi o bază de date on-line cu răspunsuri la întrebări frecvente.

5

Consola de administrare

Privire generală

BitDefender 8 Standard a fost creat cu o consolă de administrare centralizată, care permite configurarea opțiunilor de protecție pentru toate modulele BitDefender. Cu alte cuvinte, este suficient să deschideți consola de administrare pentru a avea acces la toate modulele: **Antivirus** şi **Actualizare**.

Accesul la consola de administrare se face prin meniul Windows Start, urmând calea: **Start** → **Programs** → **BitDefender 8** → **BitDefender 8 Standard**, sau mai rapid, prin dublu-clic pe icoana BitDefender din bara de sistem.

Figura 6

Din partea stângă a consolei de administrare pot fi selectate modulele BitDefender:

- ➔ General – pentru a accesa secțiunea unde veți găsi principalele setări BitDefender, detalii despre produs şi informația de contact. Tot aici puteți înregistra produsul.
- ➔ Antivirus – pentru a accesa secțiunea de configurare a modulului **Antivirus**.
- ➔ Actualizare – pentru a accesa secțiunea de configurare a modulului **Actualizare**.

Opțiunea **Ajutor**, plasată în dreapta jos, deschide documentația electronică.

Când consola este minimizată, o icoană va apărea în bara de sistem (*Figura 7*).

Figura 7

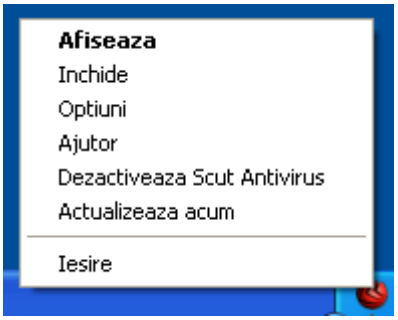


Figura 8

Dacă faceți clic dublu pe această icoană, consola de administrare se va deschide.

Dacă faceți clic-dreapta, un meniu ca cel din *Figura 8*, conținând următoarele opțiuni, va apărea:

- **Afiseaza** – deschide **consola de administrare**.
- **Inchide** – minimizează **consola de administrare** în bara de sistem.
- **Optiuni** – deschide o fereastră cu opțiunile pentru **consola de administrare**.
- **Ajutor** – deschide documentația electronică.
- **Activeaza / Dezactiveaza Scut Antivirus** – activează / dezactivează **Scutul Antivirus**.
- **Actualizeaza acum** – realizează o actualizare imediată.
- **Iesire** – închide aplicația. Selectând această opțiune, icoana din bara de sistem va dispărea iar pentru a deschide **consola de administrare** va trebui să o lansați din meniul Start.

Notă

1. Dacă dezactivați unul sau mai multe module BitDefender, icoana din bara de sistem își va schimba culoarea. Astfel puteți ști dacă anumite module sunt dezactivate fără deschiderea consolei de administrare.
2. Când există actualizări disponibile icoana va clipi.

Bara de scanare

Mulți dintre dumneavoastră ați fost probabil intrigați de "micul dreptunghi gri" pe care îl puteți muta în orice loc de pe ecran.

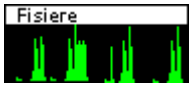


Figura 9

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

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

Notă

Atunci când **Scutul antivirus** este dezactivat veți fi notificat printr-un X roșu în zona **Fisiere** din **Bara de scanare**. Astfel puteți ști dacă sunteți protejat fără a deschide consola de administrare.

Când nu mai doriți să mai vedeți reprezentarea grafică, faceți doar clic-dreapta pe el și selectați **Inchide**.

SFAT: Pentru a ascunde bara permanent, deselectați opțiunea **Afiseaza bara de scanare** (din modulul **Antivirus**, secțiunea Scut).

Modulul General

BitDefender este configurat pentru securitate maximă. Informații generale despre toate modulele de protectie BitDefender sunt prezentate aici.

Modulul **General** conține 4 secțiuni diferite: Status, Inregistrare, Setari şi Info.

Status

Aici puteți găsi informații despre starea produsului.

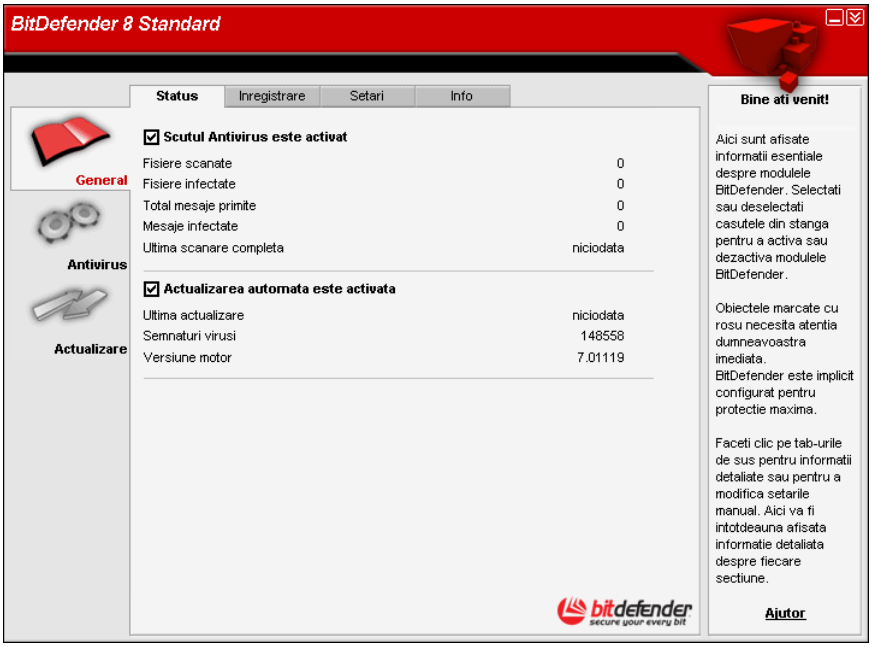


Figura 10

Selectând sau deselectând căsuțele corespunzătoare, puteți activa sau dezactiva principalele module BitDefender.

Obiectele marcate cu roşu necesită atenția dumneavoastră imediată.

Scut Antivirus

Oferă protecție continuă împotriva viruşilor şi altor programe virale, în timp real. Afişează numărul de fişiere scanate, fişiere infectate, mesaje scanate, mesaje infectate şi data ultimei scanări complete.

Pentru a preveni infecția calculatorului personal cu viruşi, păstrați **Scutul Antivirus** activat.

SFAT: Este puternic recomandată o scanare completă a sistemului cel puțin o dată pe săptămână. Pentru a rula o scanare completă, accesați modulul **Antivirus**, secțiunea Scanare, selectați **Discuri Locale** şi faceți clic pe **Scanare**.

Actualizare automată

Noi viruşi sunt descoperiți şi identificați în fiecare zi. Din acest motiv este foarte important să păstrați BitDefender la zi cu cele mai noi semnături de viruşi.

Afişează data ultimei actualizări şi numărul de viruşi care pot fi detectați (şi prin urmare dezinfectați) din baza de date BitDefender.

Pentru a vă proteja datele importante, BitDefender se poate actualiza automat. Pentru aceasta păstrați opțiunea **Actualizare automata** activată.

Înregistrare produs

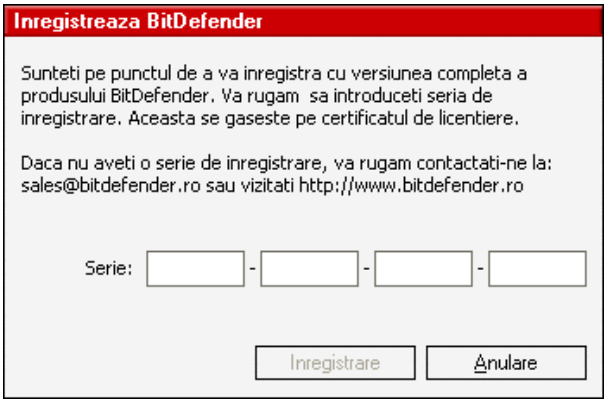
Această secțiune conține informații despre starea licenței BitDefender. Aici puteți să înregistrați produsul şi puteți afla data expirării licenței.

Figura 11

Produsul este livrat cu o serie de înregistrare validă pentru 30 de zile. La sfârşitul perioadei de evaluare, dacă doriți să folosiți produsul în continuare, trebuie să cumpărați o serie de înregistrare de la BitDefender. Faceți clic pe **Cumpara!** pentru a obține o nouă **Serie de înregistrare** din magazinul on-line BitDefender.

Pentru a modifica seria de înregistrare inițială faceți clic pe **Introduceti serie noua…**.

Următoarea fereastră va apărea:



Introduceți seria în câmpul **Serie**. Faceți clic pe **Inregistrare** pentru a încheia procesul de înregistrare.

Dacă introduceți seria greşit veți fi rugat să o reintroduceți.

Dacă introduceți o serie validă va apărea un mesaj de confirmare a succesului.

Figura 12

În secțiunea **Inregistrare** puteți afla acum data expirării noii serii de înregistrare.

SFAT: Activați produsele BitDefender cumpărate pentru a beneficia de suportul tehnic şi serviciile BitDefender în mod gratuit.

Setările consolei de administrare

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

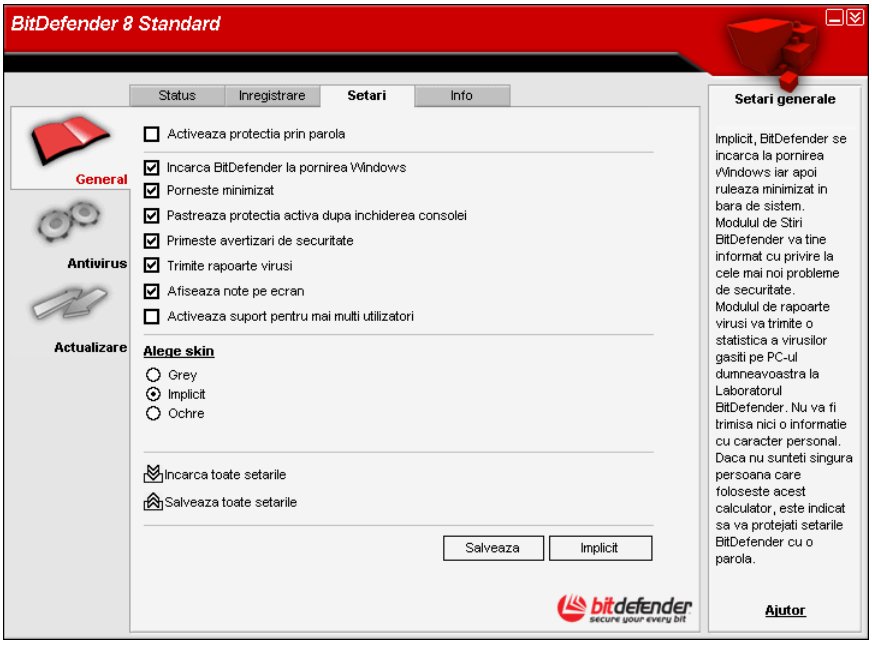


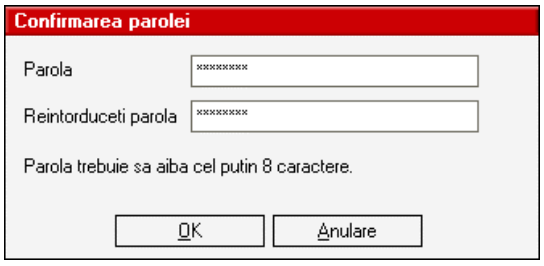
Figura 13

Pentru a selecta o opțiune, bifați pe căsuța corespondentă:

➔ **Activeaza protectia prin parola** – permite crearea unei parole pentru a proteja configurarea BitDefender.

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

Fereastra următoare va apărea:



Introduceți parola în câmpul **Parola**, reintroduceți-o în câmpul **Reintroduceti parola** şi faceți clic pe **OK**.

Figura 14

Din acest moment, dacă doriți să schimbați opțiunile de configurare ale BitDefender, veți fi rugat să introduceți parola.

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

➔ **Incarca BitDefender la pornirea Windows** – lansează BitDefender la pornirea sistemului de operare. Această opțiune este recomandată!

➔ **Porneste minimizat** – minimizează consola de administrare BitDefender după ce a fost încărcat la pornirea sistemului. Doar icoana BitDefender va apărea în bara de sistem.

- **Pastreaza protectia activa dupa inchiderea consolei** – chiar şi când consola de administrare este închisă (inclusiv din bara de sistem), BitDefender continuă să vă protejeze.
- **Primeste avertizari de securitate** – primiți din când în când notificări de securitate referitoare la noi viruşi descoperiți, trimise de serverul BitDefender.
- **Afiseaza fereastra de intampinare** – afişează fereastra care apare la lansarea BitDefender.
- **Trimite rapoarte virusi** – trimite Laboratorului BitDefender rapoarte referitoare la viruşii identificați în calculatorul dumneavoastră. Astfel ne ajutați să ținem evidența noilor viruşi.

Notă

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

- **Afiseaza note pe ecran** – afişează ferestre de informare cu privire la starea produsului.
- **Activeaza suport pentru mai multi utilizatori** – permite mai multor utilizatori ai aceluiaşi calculator sş foloseascş setşri diferite pentru BitDefender.

Notă

Această opțiune poate fi activată sau dezactivată doar de utilizatorii cu drepturi de administrator pe sistemul local.

- Opțiunea **Alege skin** vă permite să selectați culoarea consolei de administrare. Skin-ul reprezintă imaginea de fundal a interfeței. Pentru a selecta un nou skin, faceți clic pe culoarea corespunzătoare.

Folosiți butoanele **Salveaza toate setarile** / **Incarca toate setarile** pentru a salva setările BitDefender într-o anumită locație sau pentru a le încărca din această locație. Astfel, puteți folosi aceleaşi setări şi după ce ați reinstalat sau ați reparat produsul BitDefender

Apăsați pe **Salveaza** pentru a salva modificările făcute. Dacă apăsați **Implicit** veți reveni la setările implicite.

Info

În această secțiune puteți găsi informațiile de contact şi detalii despre produs.
BitDefender™ creează soluții de securitate capabile să satisfacă necesitățile de protecție ale mediului IT de azi şi oferă protecție eficientă pentru peste 38 de milioane de utilizatori individuali, cât şi mari corporații din întreaga lume, în peste 100 de țări.

BitDefender™ este certificat de către toate marile organisme de certificare independente - **ICSA Labs**, **CheckMark** şi **Virus Bulletin** şi este singurul produs de securitate care a primit un premiu **IST**.

Modulul Antivirus

BitDefender vă protejează sistemul de viruşi scanând fişierele, mesajele e-mail şi orice alte date care intră în sistem.

Caracteristici detaliate

Din modulul Antivirus aveți acces la toate setările şi caracteristicile BitDefender.

Scanare la acces sau la cerere

Scanarea antivirus se poate face în două moduri:

- Scanare la acces: Previne intrarea de noi viruşi în sistem. Această caracteristică se mai numeşte Scut Antivirus – Fişierele sunt scanate atunci când sunt accesate de către utilizator. BitDefender va scana, de exemplu, un document Word atunci când îl deschideți şi mesajele e-mail la primire. BitDefender scanează fişierele atunci când le utilizați – la acces.

- Scanare la cerere: Detectează viruşii existenți în sistem. Acesta este modul clasic de scanare, inițiată de utilizator – alegeți partițiile, directoarele sau fişierele pe care trebuie să le scaneze BitDefender, iar BitDefender le scanează – la cerere.

Explicații detaliate ale acestor tipuri de scanare pot fi găsite în capitolele următoare.

Scanarea la acces

În caz că nu ați deschis deja consola de administrare, o puteți accesa din meniul Windows Start, urmând calea: **Start** → **Programs** → **BitDefender** → **BitDefender 8 Standard** sau mai rapid, faceți dublu-clic pe icoana BitDefender din bara de sistem.

În consola de administrare, faceți clic pe **Antivirus**.

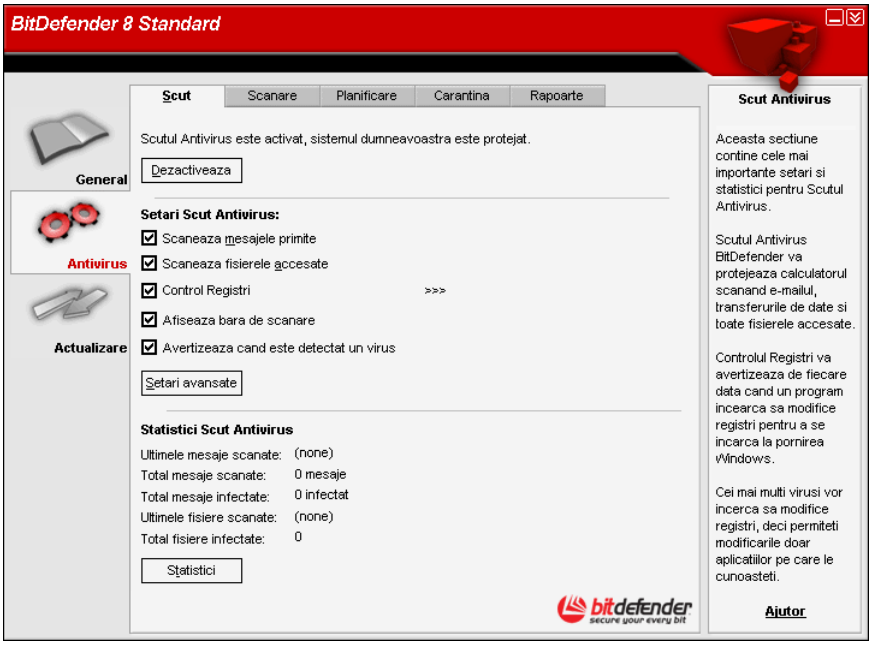


Figura 15

Scutul Antivirus vă protejează calculatorul scanând mesajele e-mail şi fişierele descărcate şi accesate.

Pentru a preveni infecția calculatorului personal cu viruşi, păstrați **Scutul Antivirus** activat.

În partea de jos a secțiunii sunt afişate statisticile BitDefender despre fişiere şi mesajele e-mail. Faceți clic pe **Statistici avansate** dacă doriți deschiderea unei ferestre cu informații detaliate despre aceste statistici.

Folosind setările puteți decide ce fişiere trebuie să scaneze BitDefender la acces şi cum ar trebui să reacționeze dacă descoperă un virus.

Control Regiştri

Una dintre părțile importante ale sistemului de operare Windows sunt regiştrii. Aici îşi păstrează Windows configurația şi setările, programele instalate, informații despre utilizator şi alte date.

Tot în regiştri sunt definite programele care sunt lansate la pornirea Windows. Viruşii folosesc des această caracteristică Windows pentru a se lansa automat atunci când utilizatorul îşi reporneşte calculatorul.

Control Regiştri supraveghează regiştrii Windows – în acest fel BitDefender poate detecta troienii. BitDefender vă va alerta de fiecare dată când un program încearcă să modifice informațiile din regiştri astfel încât să fie lansat la pornirea Windows.

Figura 16

Puteți interzice această modificare făcând clic pe **Nu** sau puteți să o permiteți făcând clic pe **Da**. Dacă doriți ca BitDefender să rețină răspunsul selectați opțiunea: **Retine acest raspuns**.

Răspunsurile dumneavoastră vor sta la baza listei de reguli.

Dacă doriți să citiți lista intrărilor în regiştri, faceți clic pe simbolul >>> corespondent **Control Registri**. Următoarea fereastră va apărea:

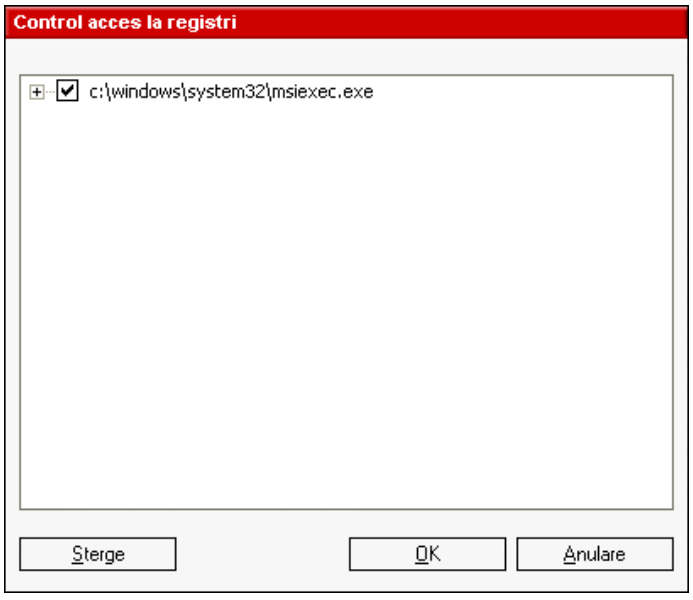


Figura 17

Pentru fiecare aplicație va fi creat un meniu expandabil; acesta conține toate modificările făcute în regiştri.

Pentru a şterge o intrare în regiştri, selectați-o şi faceți clic pe **Sterge**.

Pentru a dezactiva temporar o intrare în regiştri fără să o ştergeți, debifați căsuța corespondentă ☑ cu un clic. Când o intrare este dezactivată, căsuța corespondentă va arăta astfel: ☐.

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.

Faceți cele mai importante setări

Pentru a selecta o opțiune, doar bifați căsuța corespondentă.

- **Scaneaza mesajele primite** – toate mesajele e-mail primite vor fi scanate de BitDefender. Această opțiune este recomandată!
- **Scaneaza fisierele accesate** – toate fişierele accesate vor fi scanate de BitDefender.
- **Avertizeaza cand este detectat un virus** – o fereastră de avertizare va fi afişată la descoperirea unui virus într-un fişier sau mesaj e-mail.

  Pentru fişierele infectate fereastra de avertizare va conține calea şi numele virusului, iar pentru mesajele infectate va conține informații despre expeditor, destinatar şi numele virusului.

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

- **Afiseaza bara de scanare** – deselectați această opțiune dacă nu mai doriți afişarea barei de scanare.

Alte opțiuni

Faceți clic pe **Setari avansate** pentru a selecta obiectele pe care doriți să le scanați precum şi acțiunile ce vor fi aplicate obiectelor infectate. Următoarea fereastră va apărea:

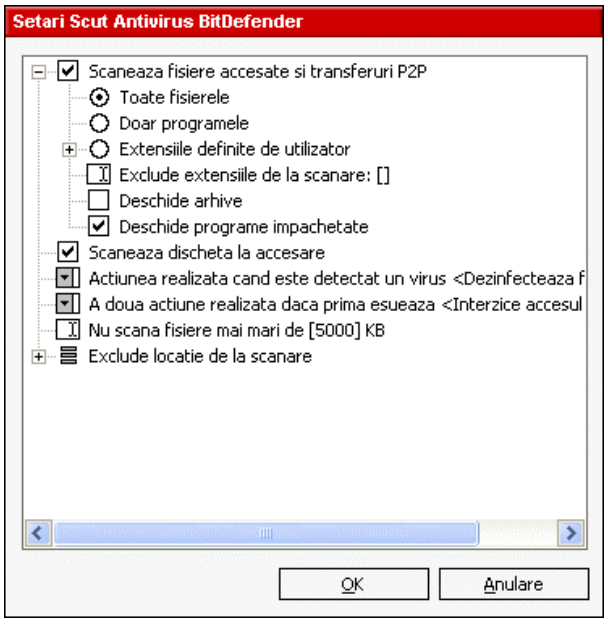


Figura 18

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

Puteți observa că unele opțiuni de scanare, deşi semnul “+” apare, nu pot fi deschise. Motivul este că aceste opțiuni nu au fost selectate încă. Veți vedea că dacă le selectați, vor putea fi deschise.

- Selectați **Scaneaza fisierele accesate si transferuri P2P** pentru a scana fişierele accesate şi comunicația prin programe de mesagerie instantă (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Pe lângă aceasta, selectați tipurile de fişiere care doriți să fie scanate.

Opțiunile următoare sunt disponibile:

Opțiune	Descriere
Toate fisierele	Toate fişierele accesate vor fi scanate, indiferent de tipurile lor.
Doar programele	Doar fişierele program vor fi scanate. Aceasta înseamnă doar fişierele cu următoarele extensii: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; 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; pfd; msi; ini; csc; cmd; bas; eml; nws.
Extensiile definite de utilizator	Doar fişierele cu extensiile specificate de utilizator vor fi scanate. Aceste extensii trebuie separate prin ";".
Exclude extensiile de la scanare	Fişierele cu extensiile specificate de utilizator NU vor fi scanate. Aceste extensii trebuie separate prin ";".
Deschide arhive	Vor fi scanate şi arhivele accesate.
Deschide programe impachetate	Programele împachetate accesate vor fi scanate.

➔ Selectați **Scaneaza discheta la accesare** dacă doriți să scanați unitatea de dischete, atunci când o folosiți.

➔ Faceți clic pe **Actiunea realizata cand este detectat un virus** şi selectați din listă prima acțiune care va fi aplicată fişierelor infectate.

BitDefender vă permite să selectați două acțiuni pentru cazul în care un virus este descoperit. A doua acțiune este activată doar dacă prima acțiune selectată este dezinfecția fişierului. Puteți selecta una dintre următoarele acțiuni:

Acțiune	Descriere
Interzice accesul si continua	În caz că un fişier este infectat, accesul la acesta va fi interzis.
Dezinfecteaza fisier	Pentru dezinfectarea fişierului.
Sterge fisier	Şterge fişierele infectate automat, fără nici un avertisment.
Muta fisier in Carantina	Fişierele infectate vor fi mutate în carantină. Atunci când sunt în carantină viruşii sunt inofensivi.

➔ Faceți clic pe săgeata corespondentă opțiunii **A doua actiune realizata daca prima esueaza** şi selectați din listă a doua acțiune pentru fişierele infectate. Sunt disponibile următoarele opțiuni:

Acțiune	Descriere
Interzice accesul si continua	În caz că un fişier este infectat, accesul la acesta va fi interzis.
Sterge fisier	Şterge fişierele infectate automat, fără nici un avertisment.
Muta fisier in Carantina	Fişierele infectate vor fi mutate în carantină. Atunci când sunt în carantină viruşii sunt inofensivi.

➔ Faceți clic pe **Nu scana fisiere mai mari de [5000] KB** şi introduceți dimensiunea maximă a fişierelor ce vor fi scanate. Dacă dimensiunea este de 0 Kb, toate fişierele vor fi scanate.

➔ Faceți clic pe semnul “+” corespondent opțiunii **Exclude locatia de la scanare** pentru a specifica un director care va fi exclus de la scanare. Prin această setare o nouă opțiune, **Obiect nou**, va apărea. Faceți clic pe căsuța corespondentă noului obiect, iar din fereastra de explorare selectați directorul pe care doriți să-l excludeți de la scanare.

Apăsați **OK** pentru a salva modificarile făcute. Dacă apăsați **Implicit** veți reveni la setările implicite.

Scanarea la cerere

Principalul obiectiv BitDefender este protejarea calculatorului dumneavoastră de viruşi. Aceasta se face în primul rând păstrând viruşii noi afară din sistem, scanând mesajele e-mail şi fişierele descărcate sau copiate pe calculator.

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

BitDefender permite patru tipuri de scanări la cerere:

- Scanare imediată – nu sunt decât câțiva paşi de urmat pentru a începe o scanare;
- Scanare contextuală – faceți clic-dreapta pe un fişier sau director şi selectați opțiunea **BitDefender Antivirus v8**;
- Scanare prin drag & drop – folosind drag & drop aduceți un fişier sau director deasupra Barei de scanare;
- Scanare programată –puteți programa BitDefender să vă scaneze sistemul de viruşi periodic.

Scanare imediată

Pentru a scana sistemul, urmați paşii:

1. Închideți toate programele

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).

2. Asigurați-vă că BitDefender recunoaşte cei mai noi viruşi

Înainte de a începe scanarea este necesar să vă asigurați că BitDefender este la zi cu semnăturile de viruşi, având în vedere că în fiecare zi se descoperă şi se identifică viruşi noi. Puteți verifica data la care a fost făcută ultima actualizare în partea de jos a modulului **Actualizare** din **Consola de administrare BitDefender**.

Dacă această dată nu este recentă, este indicat să actualizați semnăturile de viruşi ale BitDefender. Aceasta se face foarte simplu, făcând clic pe butonul **Cauta** din modulul Actualizare.

3. Alege țintele de scanare

În consola de administrare, intrați in modulul **Antivirus** şi faceți clic pe butonul **Scanare**. Secțiunea **Scanare** conține o imagine a structurii dispozitivelor de stocare din sistemul dumneavoastră. În afară de aceasta, există câteva butoane şi opțiuni de scanare.

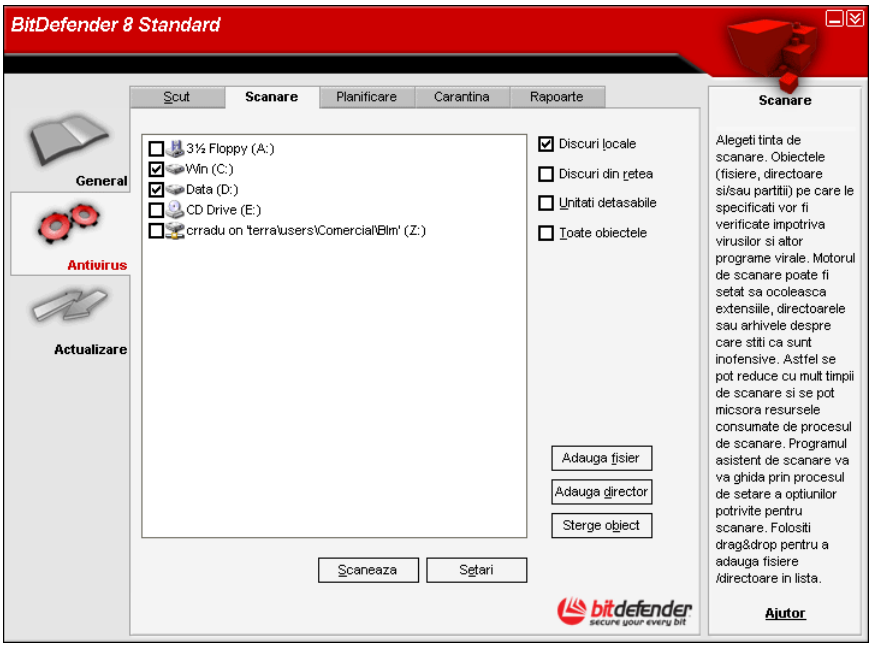


Figura 19

Secțiunea conține următoarele butoane:

- **Adauga fisiere** – deschide o fereastră de explorare în care puteți selecta fişierele pe care doriți să le scanați.
- **Adauga directoare** – deschide o fereastră de explorare în care puteți selecta directoarele care doriți să fie scanate de BitDefender.

SFAT: Puteți folosi drag & drop pentru a adăuga fişiere-directoare la listă.

- **Sterge obiecte** – şterge fişierele / directoarele care au fost selectate anterior din lista de obiecte de scanat.

Doar fişierele / directoarele adăugate de utilizator pot fi şterse, dar nu cele care au fost "văzute" automat de BitDefender.

- **Setari** – deschide o fereastră în care puteți specifica ce fişiere vor fi scanate, acțiunea de aplicat fişierelor infectate, generarea mesajelor de alertă, salvarea rezultatelor scanării in fişierele de raport.
- **Scaneaza** – lansează scanarea sistemului, luând în considerare opțiunile de scanare stabilite de utilizator.

Aceste opțiuni permit o selecție rapidă a locațiilor de scanare.

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

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

Dacă nu sunteți familiar cu calculatoarele, puteți să faceți doar clic pe butonul **Scaneaza**. BitDefender vă va scana calculatorul folosind setările standard, care sunt suficiente.

4. Selectați opțiunile de scanare – doar pentru utilizatorii avansați

Utilizatorii avansați pot folosi şi modifica opțiunile de scanare oferite de BitDefender. Motorul de scanare poate fi setat să sară peste fişierele cu anumite extensii, directoare sau arhive despre care ştiți că sunt inofensive. Aceasta poate reduce cu mult timpul de scanare, precum şi consumul din resursele sistemului.

Explorați sau modificați aceste opțiuni făcând clic pe butonul **Setari**:

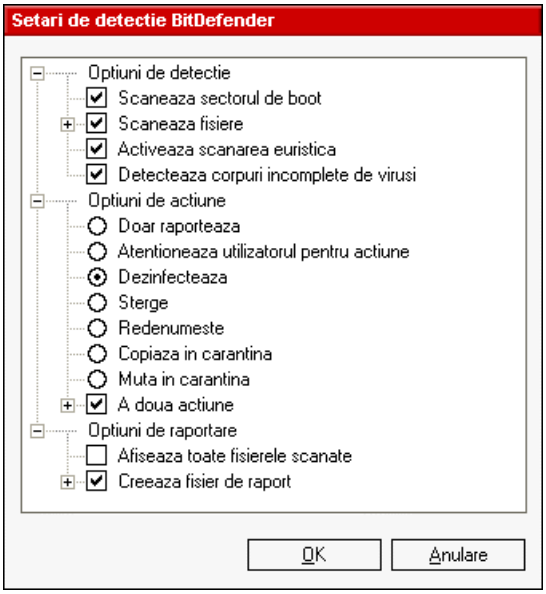


Figura 20

Opțiunile de scanare sunt organizate intr-un meniu expandabil similar celor din Windows.

Opțiunile de scanare sunt grupate în patru categorii:

- **Optiuni de detectie**
- **Optiuni de actiune**
- **Optiuni de raportare**
- **Optiuni de performanta**

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

Pasul următor constă în specificarea tipurilor de fişiere ce vor fi scanate (arhive, mesaje e-mail şi altele) şi activarea scanării euristice (pentru detecția viruşilor necunoscuți încă). Aceasta se face prin selectarea unor opțiuni din categoria **Optiuni de detectie**.

Următoarele opțiuni de detecție sunt disponibile:

Opțiune		Descriere
Scaneaza sectorul de boot		Pentru scanarea sectorului de boot.
Scaneaza fisiere	Toate fisierele	Pentru scanarea tuturor fişierelor indiferent de tipul acestora.
	Programe	Pentru scanarea doar a fişierelor program. Aceasta înseamnă doar fişierele cu următoarele extensii: `exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; 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; pfd; msi; ini; csc; cmd; bas; eml; nws.`
	Definite de utilizator	Pentru scanarea doar a fişierelor care au extensiile specificate de utilizator. Aceste extensii trebuie separate prin ";".
	Extensii excluse de la scanare	Pentru scanarea tuturor fişierelor, cu excepția celor care au extensiile specificate de utilizator. Aceste extensii trebuie separate prin ";".
	Deschide programe impachetate	Pentru scanarea programelor împachetate.
	Deschide arhive	Pentru a scana în interiorul arhivelor.
	Deschide e-mail	Pentru a scana arhivele de e-mail.
Activeaza scanarea euristica		Activează scanarea euristică a fişierelor. Scopul scanării euristice este de a identifica noi viruşi pe baza anumitor elemente şi algoritmi, înainte ca apariția lor să fie cunoscută. Întrucât această metodă nu este 100% sigură, pot apărea şi alarme false. Când un astfel de fişier este detectat, este clasificat ca suspect. În aceste cazuri, este recomandat să trimiteți fişierul la analiză către laboratorul BitDefender.
Detecteaza corpuri incomplete de virusi		Pentru a detecta şi corpuri de virus incomplete.

Mai departe, este necesar să specificați acțiunea pentru fişierele infectate sau suspecte. Faceți clic pe semnul "+" corespondent categoriei **Optiuni de actiune** pentru a deschide opțiunile şi a vedea toate acțiunile posibile pentru fişierele infectate. Puteți selecta una din următoarele opțiuni:

Opțiune	Descriere
Doar raporteaza	Pentru a raporta detectarea unui fişier infectat precum şi numele virusului.
Atentioneaza utilizatorul pentru actiune	Când este detectat un fişier infectat, va apărea o fereastră în care utilizatorul trebuie să selecteze acțiunea asupra acelui fişier. În funcție de importanța acelui fişier, puteți opta pentru dezinfectarea lui, izolarea lui în carantină sau ştergerea lui.
Dezinfecteaza	Pentru dezinfectarea fişierelor infectate.
Sterge	Pentru ştergerea fişierelor infectate.

Opțiune	Descriere
Redenumeste	Pentru schimbarea extensiilor fişierelor infectate. Noua extensie a fişierelor infectate va fi `.vir`. Prin redenumirea fişierelor infectate, posibilitatea executării lor şi prin urmare a răspândirii infecției este exclusă. De asemenea, acestea pot fi salvate pentru examinare şi analiză detaliată.
Copiaza in carantina	Pentru copierea fişierelor infectate în carantină, de unde vor putea fi trimise către laboratorul BitDefender pentru a fi analizate Aceasta înseamnă practic duplicarea fişierului infectat - prin faptul că o copie a acestui fişier va apărea în carantină şi fişierul infectat nu va fi mutat de la locația inițială.
Muta in carantina	Pentru mutarea în carantină a fişierelor infectate. Când sunt în carantină viruşii sunt inofensivi.
A doua actiune	Selectați această opțiune dacă doriți să specificați o a doua acțiune pentru fişierele infectate.

Pentru a selecta cea de-a doua acțiune pentru fişierele infectate, faceți clic pe semnul “+”, după ce ați selectat anterior opțiunea **A doua actiune**. Opțiunile disponibile pentru a doua acțiune sunt descrise in tabelul de mai jos.

Opțiune	Descriere
Doar raporteaza	Pentru a raporta detectarea unui fişier infectat precum şi numele virusului.
Atentioneaza utilizatorul pentru actiune	Când este detectat un fişier infectat, va apărea o fereastră în care utilizatorul trebuie să selecteze acțiunea asupra acelui fişier. În funcție de importanța acelui fişier, puteți opta pentru dezinfectarea lui, izolarea lui în carantină sau ştergerea lui.
Sterge	Pentru ştergerea fişierelor infectate.
Redenumeste	Pentru schimbarea extensiilor fişierelor infectate. Noua extensie a fişierelor infectate va fi `.vir`. Prin redenumirea fişierelor infectate, posibilitatea executării lor şi prin urmare a răspândirii infecției este exclusă. De asemenea, acestea pot fi salvate pentru examinare şi analiză detaliată.
Copiaza in carantina	Pentru copierea fişierelor infectate în carantină, de unde vor putea fi trimise către laboratorul BitDefender pentru a fi analizate Aceasta înseamnă practic duplicarea fişierului infectat - prin faptul că o copie a acestui fişier va apărea în carantină şi fişierul infectat nu va fi mutat de la locația inițială.
Muta in carantina	Pentru mutarea în carantină a fişierelor infectate. Când sunt în carantină viruşii sunt inofensivi.

Următorul pas constă în selectarea opțiunilor de raportare. Pentru aceasta va trebui să faceți clic pe semnul “+” corespondent categoriei **Optiuni de raportare**. Aceste opțiuni permit crearea unui fişier de raport (fişier care conține informații despre procesul de scanare).

Opțiune		Descriere
Afiseaza toate fisierele scanate		Listează toate fişierele scanate (infectate sau nu) şi starea acestora în fişierul de raport. Această opțiune vă va încetini calculatorul.
Creeaza fisier de raport	Creeaza fisier de raport <vscan.log>	Acesta este practic un câmp de editare care permite schimbarea numelui fişierului de raport. Trebuie să faceți doar clic pe această opțiune şi să introduceți un nou nume.
	Adauga la raportul existent	Selectați această opțiune dacă doriți să adăugați informațiile despre noua scanare la cele deja existente în fişierul de raport. Se realizează astfel un mic istoric.
	Limiteaza marimea fisierului de raport la [0] KB	Faceți clic pe această opțiune şi introduceți dimensiunea maximă a fişierului de raport în câmpul de editare care apare.

În categoria **Optiuni de performanta** puteți reduce prioritatea procesului de scanare. Dacă selectați opțiunea **Executa procesul cu prioritate joasa** veți permite altor programe să ruleze cu o viteză superioară dar timpul necesar pentru finalizarea scanării va creşte.

Aceste fişiere de raport pot fi vizualizate în secțiunea Rapoarte din modulul **Antivirus**.

Notă

Puteți observa că anumite opțiuni de scanare, deşi semnul "+" apare în dreptul lor, nu pot fi expandate. Motivul este că aceste opțiuni nu au fost selectate încă. Veți observa că dacă le selectați, ele vor putea fi expandate.

Apăsați **OK** pentru a salva modificările făcute. Dacă apăsați **Implicit** veți reveni la setările implicite.

5. Lansarea scanării

Având selectate opțiunile de scanare, tot ce trebuie să faceți este să porniți scanarea sistemului. Pentru aceasta, faceți clic pe **Scaneaza**. Lansarea poate lua ceva timp, în funcție de dimensiunea discului dumneavoastră.

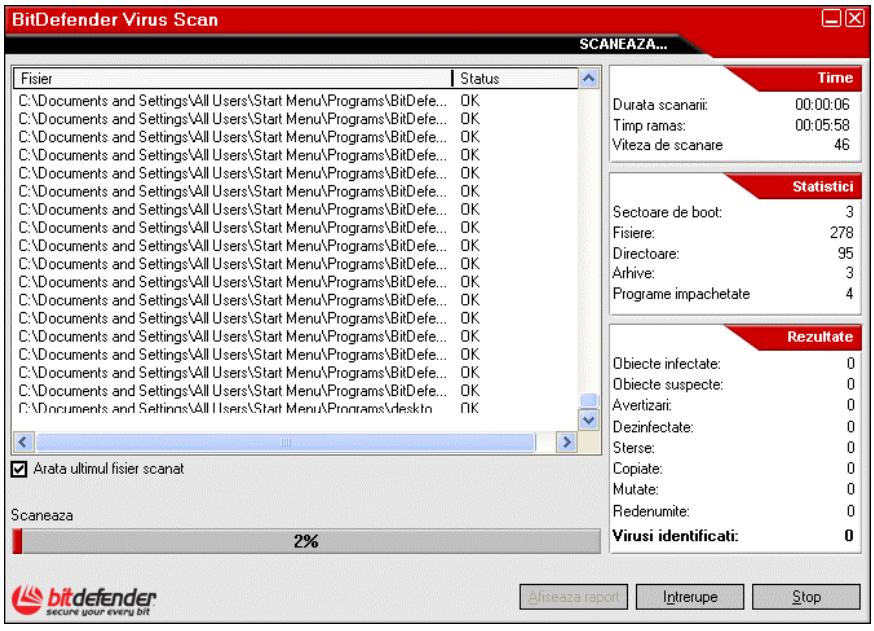


Figura 21

În timpul scanării, BitDefender va afişa progresul scanării şi vă va alerta dacă descoperă viruşi.

Selectați opțiunea **Arata ultimul fisier scanat** şi doar informația despre ultimul fişier scanat va fi vizibilă.

Dacă faceți clic pe:

- **Stop** - va apărea o fereastră nouă care vă permite oprirea verificării sistemului. Dacă alegeți să opriți verificarea, butonul **Stop** se va transforma în **Inchide**, iar dacă faceți clic pe acesta fereastra de scanare se va închide.
- **Intrerupe** - scanarea se va opri temporar - o puteți relua apăsând butonul **Reia**.
- **Afiseaza raport** - se va deschide raportul de scanare.

Fişierul de raport este salvat automat în secțiunea Rapoarte din modulul **Antivirus**.

Pentru a putea observa ce fişiere sunt scanate trebuie să aveți selectată opțiunea **Afiseaza toate fisierele scanate**. Aceasta o găsiți la **Optiuni de raportare**, din secțiunea Selectarea optiunilor de scanare. Această opțiune vă va încetini calculatorul.

6. Metode alternative de scanare

BitDefender oferă două metode alternative de scanare imediată a fişierelor: folosind meniul contextual şi folosind drag & drop.

Scanare contextuală

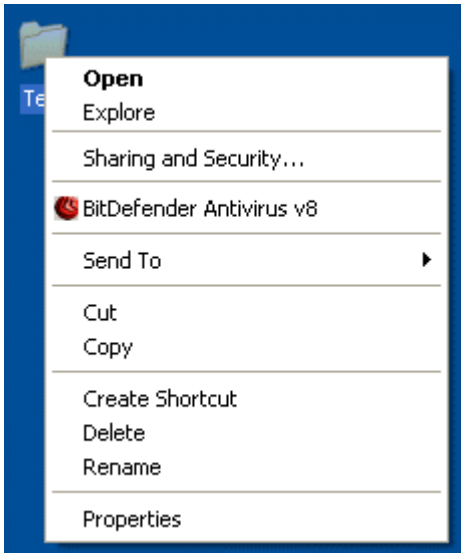


Figura 22

Faceți clic-dreapta pe fişierul sau directorul pe care doriți să-l scanați şi selectați opțiunea **BitDefender Antivirus v8**.

Va fi creat un fişier de raport `vscan.log` pe care îl puteți vizualiza în modulul **Antivirus**, secțiunea Rapoarte.

Scanare prin drag & drop

Folosind drag & drop, trageți fişierul sau directorul pe care doriți să îl scanați peste **Bara de scanare**, ca în imaginile de mai jos.

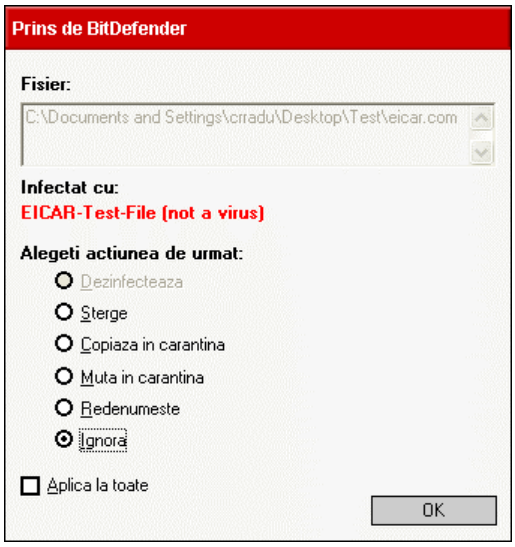
Figura 23

Figura 24

Va fi creat un fişier de raport `activbar.log` pe care îl puteți vizualiza în modulul **Antivirus**, secțiunea Rapoarte.

În ambele cazuri fereastra de scanare (*Figura 21*) va apărea.

Dacă un virus este detectat, o fereastră de alertă va apărea.



Puteți afla numele fişierului infectat, precum şi numele virusului.

Figura 25

Puteți selecta una dintre următoarele acțiuni pentru fişierul infectat:

- **Dezinfecteaza** - pentru dezinfectarea fişierelor infectate.
- **Sterge** – pentru ştergerea fişierelor infectate.
- **Copiaza in carantina** – pentru copierea fişierelor infectate în carantină.
- **Muta in carantina** – pentru mutarea fişierelor infectate în carantină.
- **Redenumeste** – pentru schimbarea extensiilor fişierelor infectate. Noua extensie a fişierelor infectate va fi `.vir`.
- **Ignora** – pentru a ignora fişierele infectate. Nici o acțiune nu va fi aplicată fişierelor infectate.

Dacă scanați un director şi doriți ca acțiunea să fie la fel pentru toate fişierele infectate, selectați opțiunea **Aplica la toate**.

Dacă opțiunea **Dezinfecteaza** nu poate fi selectată, înseamnă că tentativa BitDefender de a dezinfecta fişierul a eşuat. Cea mai bună soluție este izolarea virusului în carantină si trimiterea pentru analiză la Laboratorul BitDefender.

La sfârşit, faceți clic pe **OK**.

Scanarea programată

Având în vedere că procesul de scanare necesită timp şi necesită închiderea tuturor programelor, este cel mai bine să programați scanarea într-un moment când nu vă folosiți calculatorul. Aceasta necesită crearea de către utilizator a unui eveniment de scanare programat.

Acesta are următoarele caracteristici:

- Un program asistent ce ajută la crearea evenimentelor programate de scanare;
- Posibilitatea de selectare a frecvenței de scanare;
- Selectarea fişierelor şi / sau a directoarelor;
- Selectarea extensiilor de fişiere;
- Modul de configurare separată a fiecărui eveniment de scanare;
- Posibilități de scanare în LAN;
- Izolarea automată a fişierelor infectate sau suspecte în carantină;
- Scanare în background, fără a interfera cu activitatea curentă a utilizatorului;
- Sumarul proprietăților evenimentului de scanare;
- Generarea de rapoarte de scanare.

În consola de administrare, intrați în modulul **Antivirus** şi faceți clic pe tab-ul **Planificare**.

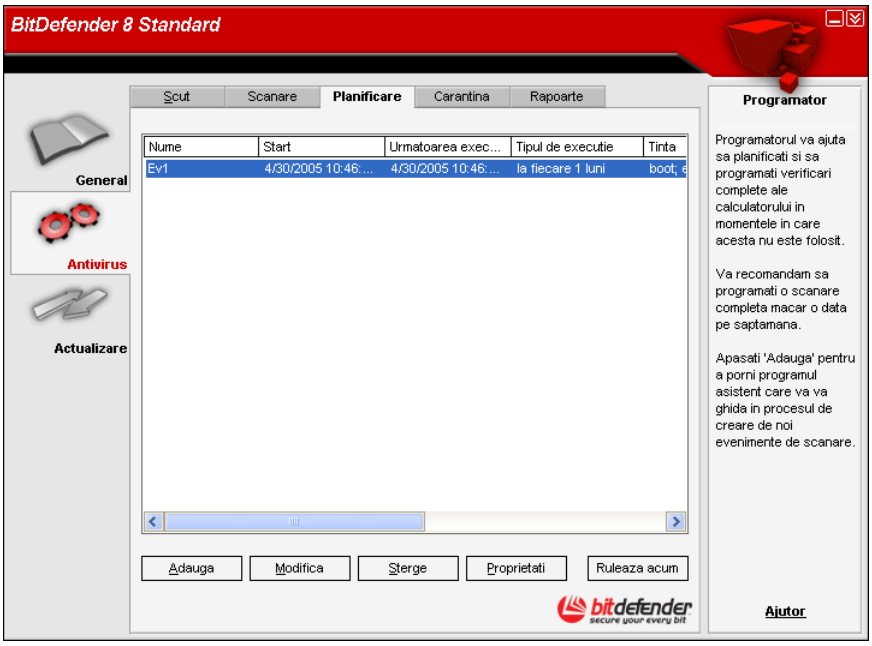


Figura 26

Aceasta secțiunea conține câteva butoane pentru administrarea evenimentelor de scanare:

➔ **Adauga** – lansează programul asistent care vă va ghida prin procesul de creare al unui nou eveniment de scanare.
➔ **Modifica** – modifică proprietățile unui eveniment creat anterior. Aceasta se face de asemenea prin lansarea programului asistent.

Dacă modificați numele evenimentului, un nou eveniment va fi creat, cu numele nou introdus.

➔ **Sterge** – şterge evenimentul selectat.

➔ **Proprietati** – afişează proprietăţile evenimentului selectat.
➔ **Ruleaza acum** – începe rularea evenimentului.

Secţiunea **Planificare** conţine şi o listă în care pot fi văzute toate evenimentele de scanare, numele acestora, data primei execuţii, data următoarei execuţii şi tipul scanării (periodică sau o singură dată).

Secţiunea **Planificare** dispune de un program asistent pentru crearea evenimentelor de scanare. El vă va oferi asistenţă de fiecare dată când doriţi să efectuaţi o operaţie cu aceste evenimente de scanare, indiferent dacă este vorba de crearea unuia nou sau modificarea unuia deja creat.

Faceţi clic pe **Adauga**. Aceasta va lansa programul asistent de creare a unui nou eveniment de scanare.

Este puternic recomandat să programaţi cel puţin o scanare săptămânală.

1. Specificarea numelui evenimentului de scanare

Primul pas constă în specificarea unui nume pentru noul eveniment.

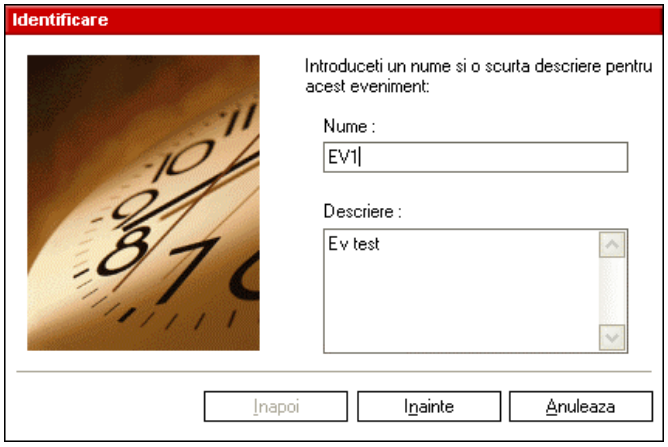


Figura 27

Introduceţi numele noului eveniment în câmpul **Nume** şi o scurtă descriere în câmpul **Descriere**.

Selectaţi opţiunea **Acest proces are prioritate scazuta** dacă doriţi să reduceţi prioritatea evenimentului de scanare şi să permiteţi altor programe să ruleze mai repede. Aceasta va creşte timpul necesar pentru finalizarea scanării.

Faceţi clic pe **Inainte** pentru a trece la pasul următor. Dacă faceţi clic **Anulare** va apărea o fereastră care vă va cere confirmarea opţiunii: părăsirea programului asistent sau continuarea procesului.

2. Selectarea frecvenţei de scanare

În continuare va apărea o fereastră în care va trebui să selectaţi tipul scanării:

Selectaţi căsuţa corespondentă opţiunii **O singura data** dacă doriţi să creaţi un eveniment care să ruleze o singură dată.

Dacă doriţi ca evenimentul să fie repetat la o anumită perioadă, selectaţi căsuţa corespondentă opţiunii **Periodic**.

Figura 28

Introduceți în câmpul de editare **La fiecare** numărul de minute / ore / zile / săptămâni / luni / ani la care doriți să se repete evenimentul.

Puteți utiliza butoanele sus / jos pentru a mări / micşora numărul de minute / ore / zile / săptămâni / luni / ani.

Selectați intervalul - minute, ore, zile, săptămâni, luni, ani – la care doriți ca evenimentul de scanare să se repete. Desfăşurați lista de la săgeată şi selectați unitatea de timp pe care o doriți.

Dacă ați optat pentru un eveniment periodic, acesta va fi repetat la perioada de timp selectată până când va fi şters din lista de evenimente a secțiunii **Planificare**.

După ce ați selectat perioada, faceți clic pe **Inainte** pentru a trece la pasul următor. Dacă doriți să reveniți la pasul anterior, faceți clic pe **Inapoi**.

3. Selectarea obiectelor de scanat

Următorul pas constă în selectarea obiectelor pe care doriți să le scanați - sectorul de boot, fişierele, mail-urile, arhivele, programele împachetate.

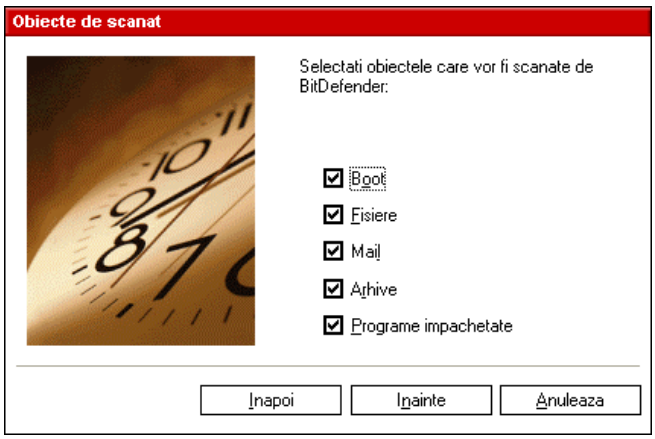


Figura 29

Selectați unul sau mai multe obiecte de scanat prin simpla selectare a celor pe care le doriți.

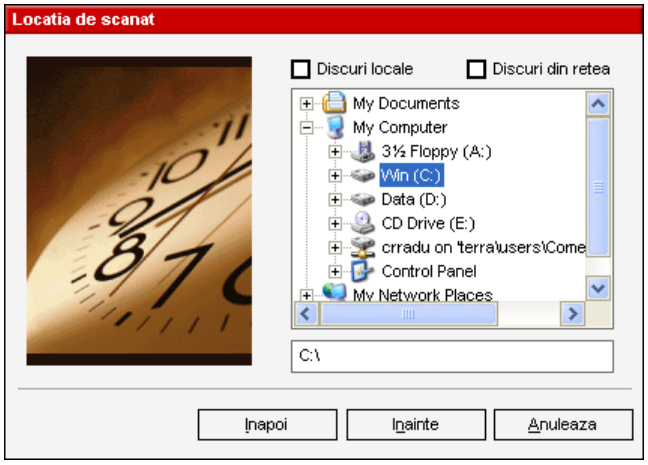
Puteți selecta dintre următoarele obiecte:

- **Boot** – pentru a scana sectorul de boot;
- **Fisiere** – pentru a scana fişierele;
- **Mail** – pentru a scana arhivele de mail pentru detectarea viruşilor;
- **Arhive** – pentru a scana în arhive;
- **Programe impachetate** – pentru a scana fişierele împachetate.

Faceți clic pe **Inainte**.

4. Selectarea locației de scanat

În continuare va trebui să specificați calea către obiectele care să fie scanate, după cum se poate observa şi din imagine. Acest pas este necesar dacă ați selectat la pasul anterior să fie scanate fişierele.



Această secțiune este de fapt o fereastră de explorare în care puteți selecta partițiile şi directoarele care să fie scanate.

Când cursorul este plasat pe un director, calea completă către acesta va apărea în câmpul plasat sub această fereastră de explorare.

Figura 30

Faceți clic pe semnul "+" pentru a expanda o opțiune sau pe cea cu semnul "-" pentru a restrânge o opțiune.

De asemenea, pentru selectarea locațiilor care să fie scanate, puteți să folosiți opțiunile de selectare rapidă plasate în partea de sus a secțiunii:

- **Discuri locale** – pentru a scana partițiile locale;
- **Discuri din retea** – pentru a scana locațiile din rețea recunoscute.

Faceți clic pe **Inainte**.

5. Selectarea tipurilor de fişiere

Specificați tipurile de fişiere care vor fi scanare.

Acest pas este necesar doar dacă ați ales să scanați fişiere.

Figura 31

Puteți selecta:

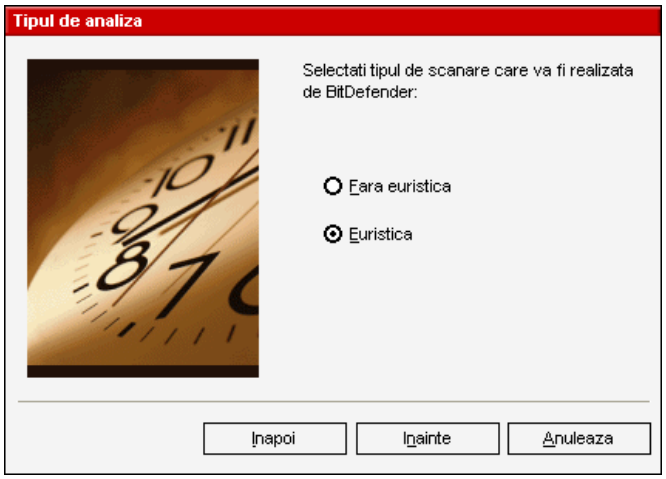
- **Toate** – pentru a scana toate fişierele, indiferent de tipul lor;
- **Executabile si documente** – pentru a scana fişierele program şi documentele;
- **Din lista** – pentru a scana doar fişierele ale căror extensii apar în listă. Aceste extensii trebuie separate prin ";".

Dacă doriți să vedeți informații despre fişierele scanate, infectate sau nu, selectați opțiunea **Afiseaza toate fisierele scanate**.

Faceți clic pe **Inainte**.

6. Selectarea tipului de analiză

Selectați tipul de analiză.



Aceasta, după cum se observă din imagine, implică alegerea între două tipuri de analiză:

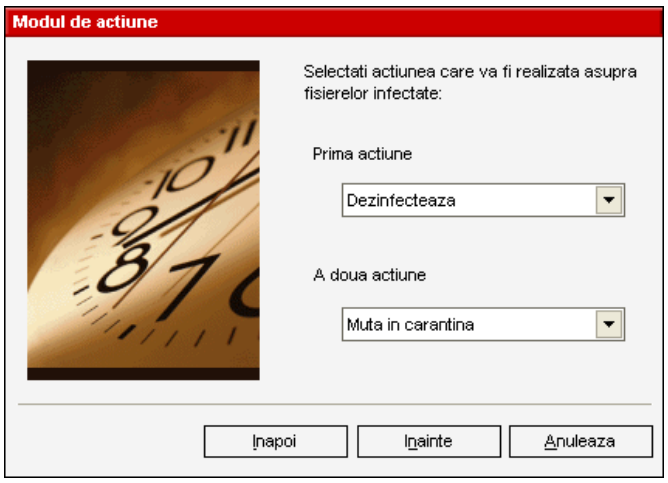
Figura 32

- **Scanare euristica** – reprezintă o metodă bazată pe anumiți algoritmi, al cărei scop este să identifice noi viruşi, necunoscuți încă. Ocazional poate raporta cod suspicios în programele normale, generând aşa-numitul "fals pozitiv". Pentru a activa acest tip de scanare, selectați opțiunea **Euristica**;
- **Scanare non-euristica** - înseamnă scanarea fişierelor pe baza unor semnături de viruşi deja cunoscuți. Pentru a selecta acest tip de scanare, faceți clic pe opțiunea **Fara euristica.**

Faceți clic pe **Inainte**.

7. Selectarea acțiunii asupra fişierelor infectate

BitDefender permite selectarea a două acțiuni în cazul în care un virus este găsit.



Vă recomandăm să alegeți **Dezinfecteaza** pentru prima acțiune şi **Muta in carantina** pentru a doua acțiune.

Figura 33

Pentru prima acțiune poate fi selectată una dintre următoarele opțiuni:

Acțiune	Descriere
Dezinfecteaza	Pentru a dezinfecta fişierele infectate.
Sterge	Pentru a şterge automat, fără nici un avertisment toate fişierele infectate. Acțiune nerecomandată!
Muta in Carantina	Pentru a muta fişierele infectate din locația inițială în zona de carantină. Când sunt în carantină viruşii sunt inofensivi.
Redenumeste	Pentru a schimba extensiile fişierelor infectate. Noua extensie a fişierelor infectate va fi `.vir`. Redenumind fişierele infectate riscul răspândirii infecției prin executarea lor este eliminat. Astfel ele pot fi păstrate pentru a fi examinate şi analizate.
Intreaba utilizatorul	De fiecare dată când un virus este detectat, o fereastră de alertă va apărea utilizatorul având posibilitatea de a selecta acțiunea ce va fi realizată. Este recomandat ca la alegerea acțiunii să considerați importanța fişierului.
Ignora	În acest caz infecția va fi ignorată şi nu se va realiza nici o acțiune. Se va raporta doar existența virusului.

Selectați a doua acțiune pentru a fi realizată dacă prima eşuează:

Opțiune	Descriere
Sterge	Pentru a şterge automat, fără nici un avertisment toate fişierele infectate.
Muta in Carantina	Pentru a muta fişierele infectate din locația inițială în zona de carantină. Când sunt în carantină viruşii sunt inofensivi.
Redenumeste	Pentru a schimba extensiile fişierelor infectate. Noua extensie a fişierelor infectate va fi `.vir`. Redenumind fişierele infectate riscul răspândirii infecției prin executarea lor este eliminat. Astfel ele pot fi păstrate pentru a fi examinate şi analizate.
Intreaba utilizatorul	De fiecare dată când un virus este detectat, o fereastră de alertă va apărea utilizatorul având posibilitatea de a selecta acțiunea ce va fi realizată. Este recomandat ca la alegerea acțiunii să considerați importanța fişierului.
Ignora	În acest caz infecția va fi ignorată şi nu se va realiza nici o acțiune. Se va raporta doar existența virusului.

Faceți clic pe **Inainte**.

8. Raportare

Setați opțiunile de creare a fişierului de raport.

Figura 34

Pentru a crea un raport de scanare, selectați opțiunea **Creeaza fisier de raport**. În acest moment toate celelalte opțiuni pentru crearea fişierului de raport vor fi activate.

Introduceți numele fişierului de raport în câmpul **Nume fisier de raport**. Numele implicit este `schedule.log`. Raportul va conține informații despre procesul de scanare: numărul de viruşi identificați, numărul de fişiere scanate, numărul de fişiere dezinfectate şi de fişiere şterse.

Faceți clic pe **Adauga** dacă doriți să adăugați informațiile despre noua scanare la un raport deja existent, generând astfel un scurt istoric al scanărilor din diferite momente.

Faceți clic pe **Suprascrie** dacă doriți să creați un nou fişier de raport la fiecare scanare. În acest caz informațiile despre scanarea anterioară vor fi pierdute.

SFAT: Puteți vizualiza fişierul de raport în secțiunea Rapoarte din modulul **Antivirus**.

Faceți clic pe **Inainte**.

9. Rezumat

Acesta este ultimul pas din procesul de creare a unui eveniment de scanare.

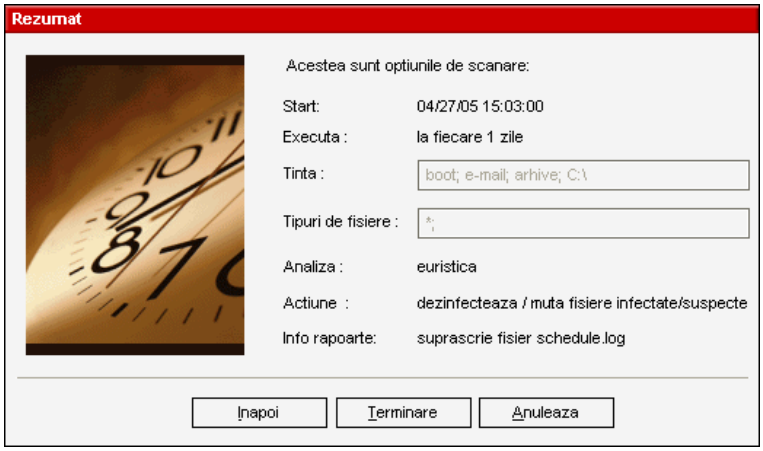


Figura 35

În această fereastră puteți vedea toate setările pentru evenimentul de scanare şi puteți face modificări, revenind la paşii anteriori (**Inapoi**). Dacă nu doriți să faceți modificări, faceți clic pe **Terminare**.

Noul eveniment va apărea în secțiunea **Planificare**.

În lista secțiunii **Planificare** puteți afla pentru fiecare eveniment de scanare planificat, numele, descrierea, data de lansare, data următoarei lansări, tipul evenimentului (o singură dată sau periodic), ținta de scanare, extensiile fişierelor de analizat, tipul de analiză şi acțiunea de realizat când un virus este descoperit.

Notă

La modificarea unui eveniment de scanare vor fi urmați aceiaşi paşi ca la creare. Dacă modificați numele evenimentului va fi creat un nou eveniment. De exemplu, dacă avem evenimentul EV1 şi îi modificăm numele în EV2, EV1 nu va dispărea, dimpotrivă, va apărea un nou eveniment, EV2, cu aceleaşi proprietăți ca EV1.

Dacă faceți clic-dreapta pe un eveniment de scanare din listă, un meniu, ca cel din poza de mai jos va apărea:

Figura 36

Dacă nu este selectat nici un eveniment şi faceți clic-dreapta în secțiunea **Planificare**, va fi activă doar opțiunea **Adauga**, celelalte fiind dezactivate.

SFAT: Modulul **Planificare** permite existenta oricâtor evenimente de scanare.

Puteți naviga prin evenimentele de scanare folosind tastatura: apăsați tasta **Delete** pentru a şterge evenimentul selectat, apăsați pe tasta **Enter** pentru a vizualiza proprietățile evenimentului selectat sau apăsați pe tasta **Insert** pentru a adăuga un nou eveniment (va apărea programul asistent al modulului **Planificare**).

Folosiți săgețile de la tastatură pentru a naviga în sus, jos, la dreapta sau la stânga în lista cu evenimente de scanare.

Izolarea fişierelor infectate

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

Componenta BitDefender care asigură administrarea fişierelor izolate este modulul **Carantina**. Acest modul a fost creat cu posibilitatea de a trimite automat fişierele infectate la Laboratorul BitDefender.

În caz că nu ați deschis deja consola de administrare, o puteți accesa din meniul Windows Start, urmând calea **Start** → **Programs** → **BitDefender** → **BitDefender 8 Standard** sau mai rapid, faceți dublu-clic pe icoana BitDefender din bara de sistem.

În consola de administrare, intrați în modulul **Antivirus** şi faceți clic pe tab-ul **Carantina**.

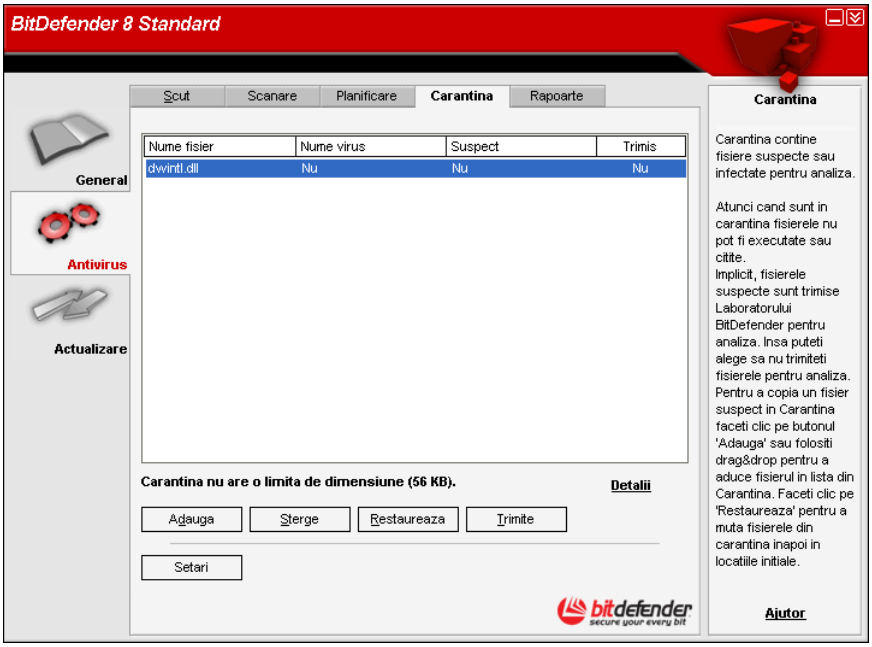


Figura 37

După cum puteți observa, secțiunea **Carantina** conține o listă cu toate fişierele care au fost izolate până acum. Fiecărui fişier i se poate afla numele, dimensiunea, data izolării şi data trimiterii. Dacă doriți mai multe informații despre fişierele din carantină faceți clic pe **Detalii**.

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

Secțiunea **Carantina** conține câteva butoane pentru administrarea fişierelor:

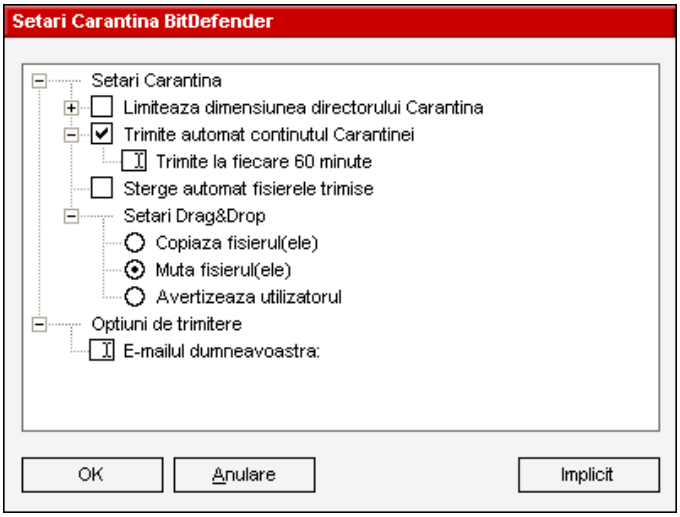
➔ **Adauga** – adaugă fişiere în carantină. Folosiți acest buton pentru a băga în carantină fişiere pe care le suspectați că sunt infectate. Se va deschide o fereastră în care puteți selecta fişierul din locația în care se află pe disc. În acest fel fişierul va fi copiat în carantină. Dacă doriți să mutați fişierul în zona de carantină selectați opțiunea **Sterge din locatia originala**. O metodă mai rapidă prin care puteți adăuga fişiere în carantină este folosirea drag & drop pentru a le aduce în listă.

- **Sterge** – şterge din calculator fişierele selectate.
- **Restaureaza** – mută fişierul în locația sa inițială.
- **Trimite** – trimite fişierele selectate la Laboratorul BitDefender pentru analiză detaliată. Înainte de a trimite fişierele trebuie să specificați anumite informații. Pentru aceasta faceți clic pe **Setari** şi completați câmpurile din secțiunea **Setari e-mail**, după indicațiile de mai jos.

Notă

Fişierele suspecte sunt trimise implicit Laboratorului BitDefender. Însă puteți opta să nu trimiteți fişierele pentru analiză selectând opțiunea **Trimite automat continutul Carantinei** din **Setari Carantina**.

- **Setari** – deschide opțiunile avansate pentru zona de carantină. Va apărea următoarea fereastră:



Opțiunile carantinei sunt grupate în două categorii:

- **Setari Carantina**
- **Opțiuni de trimitere**

Faceți clic pe semnul "+" pentru a deschide o opțiune sau pe "-" pentru a închide o opțiune.

Figura 38

Setari Carantina

- **Limiteaza dimensiunea directorului Carantina** – păstrează dimensiunea carantinei sub control. Această opțiune implicit activată având dimensiunea setată la 12000 KB. Dacă doriți să modificați această valoare puteți introduce valoarea dorită în câmpul **Dimensiunea maxima a directorului Carantina este**.

  Opțiunea **Sterge automat fisierele vechi** este utilă pentru a şterge fişierele vechi atunci când carantina este plină şi nu mai este spațiu pentru alte fişiere.

- **Trimite automat continutul Carantinei** – trimite automat fişierele din carantină Laboratorului BitDefender pentru analiză aprofundată. Puteți seta perioada de timp dintre două procese de trimitere în câmpul **Trimite la fiecare 60 minute**.
- **Sterge automat fisierele trimise** – şterge automat fişierele din carantină după ce au fost trimise la Laboratorul BitDefender.
- **Setari Drag & Drop** – dacă folosiți metoda Drag & Drop pentru a adăuga fişiere în carantină, aici puteți specifica acțiunea pe care doriți să o realizați: copiază fişierele, muta fişierele sau avertizează utilizatorul.

Opțiuni de trimitere

Pentru a trimite fişiere la Laboratorul BitDefender trebuie specificată adresa e-mail.

- **E-mailul dumneavoastra** – introduceți adresa de e-mail dacă doriți să primiți informații despre fişierele suspecte pe care le-ați trimis la analiză.

Vizualizarea fişierelor de raport

La lansarea unui proces de scanare, utilizatorul poate opta pentru crearea unui fişier de raport în care va putea găsi informații despre procesul de scanare. Utilizatorul poate vizualiza aceste rapoarte direct din consola de administrare.

În caz că nu ați deschis deja consola de administrare, o puteți accesa din meniul Windows Start, urmând calea **Start** → **Programs** → **BitDefender** → **BitDefender 8 Standard** sau mai rapid, faceți dublu-clic pe icoana BitDefender din bara de sistem.

În consola de administrare, intrați în modulul **Antivirus** şi faceți clic pe tab-ul **Rapoarte**.

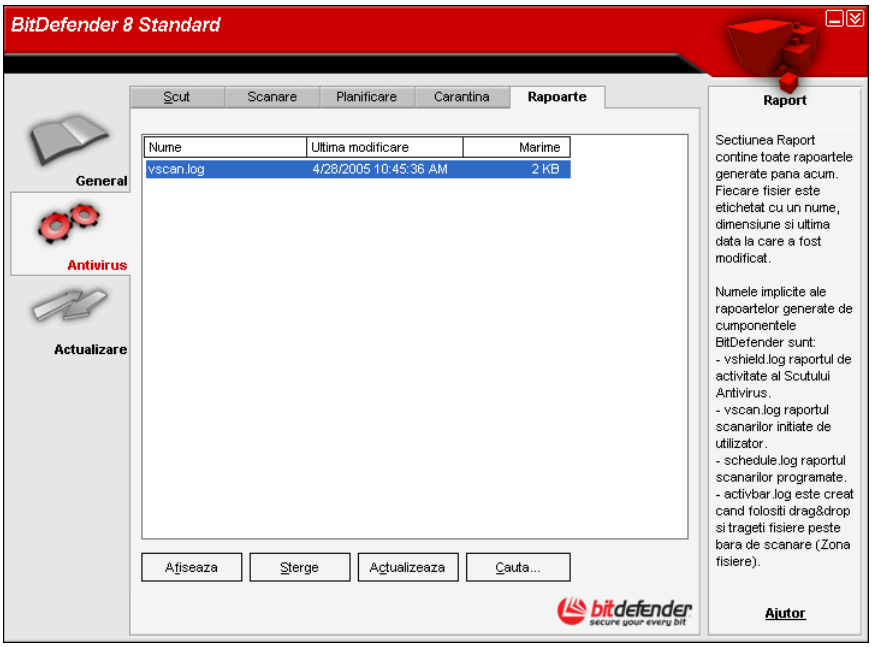


Figura 39

BitDefender va ține o evidență a activității sale pe calculatorul dumneavoastră. Fişierele de raport sunt următoarele:

- Vshield.log este raportul pe care BitDefender îl scrie în timpul scanării protecției mesajelor de e-mail cât şi a programelor active de pe sistemul dumneavoastră;
- Vscan.log este scris când efectuați o scanare imediată a sistemului;
- Schedule.log conține informații despre scanările programate;
- Activbar.log este creat când scanați folosind drag & drop.

Secțiunea **Rapoarte** conține o listă cu toate fişierele de raport scrise. Pentru fiecare fişier este afişat numele, dimensiunea şi data ultimei modificări. Secțiunea include şi butoane pentru administrarea fişierelor de raport.

Funcțiile butoanelor sunt explicate mai jos:

- **Afiseaza** – deschide fişierul de raport selectat.
- **Sterge** – şterge fişierul de raport selectat.
- **Actualizeaza** – dacă în timp ce consola de administrare este deschisă la secțiunea **Rapoarte** iar în acelaşi timp realizați o scanare a calculatorului, noul raport cu rezultatele scanării (dacă ați selectat opțiunea **Creeaza fisier de raport**) va fi vizibil doar după ce faceți clic pe **Actualizeaza**.
- **Cauta…** – deschide o fereastră în care puteți selecta fişierele de raport pe care doriți să le vizualizați.

SFAT: Fişierele de raport sunt salvate implicit în directorul în care este instalat BitDefender. Dacă ați salvat fişiere de raport într-un alt director, trebuie să folosiți butonul **Cauta** pentru a le localiza.

Eliminarea viruşilor

Este mult mai uşor să împiedicați un virus să intre în sistem, decât să îi eliminați după ce v-au infectat calculatorul. Din acest motiv protecția de viruşi ar trebui să fie tot timpul activată şi actualizată.

Dacă BitDefender detectează un virus rezident este recomandat să permiteți BitDefender să încerce eliminarea acestuia. Această operație poate însă eşua din diverse motive – viruşii rezidenți, deja activi în sistemul dumneavoastră, pot fi foarte dificil de eliminat.

Dacă BitDefender detectează un virus dar nu reuşeşte să vă curețe sistemul este recomandat să contactați echipa noastră de suport pe adresa suport@bitdefender.ro.

Secretul pentru eliminarea unui virus este să ştii totul despre el. Puteți găsi informații suplimentare referitoare la viruşi pe site-ul nostru, www.bitdefender.ro.

Pentru viruşii cu cea mai mare răspândire am creat programe speciale de eliminare.

Este întotdeauna folositor să căutați pe Internet informații detaliate despre virusul în cauză.

Pentru mai mult ajutor contactați echipa noastră pentru suport gratuit la adresa suport@bitdefender.ro.

Modulul Actualizare

Noi viruşi sunt descoperiți şi identificați în fiecare zi. Din acest motiv este foarte important să țineți BitDefender la zi cu toate semnăturile de viruşi. Implicit, BitDefender caută actualizări automat la fiecare trei ore.

Caracteristici

Actualizările sunt de trei tipuri:

- **Actualizare de produs** – la lansarea unei noi versiuni de produs, noi caracteristici şi tehnici de scanare sunt introduse pentru a îmbunătăți performanțele produsului. Acest tip de actualizare se mai numeşte **Product Update**;
- **Actualizări pentru motoarele Antivirus** – pentru că noi viruşi apar tot timpul, fişierele care conțin semnăturile de viruşi trebuiesc actualizate pentru a asigura protecție permanentă, la zi, împotriva acestora. Acest tip de actualizare se mai numeşte **Virus Definitions Update**.

În ceea ce priveşte intervenția utilizatorului, putem considera următoarele tipuri de actualizări:

- **Actualizare manuală** – căutarea de actualizări la cererea utilizatorului;
- **Actualizare automată** – antivirusul contactează automat serverul BitDefender pentru a verifica dacă o nouă actualizare este disponibilă. Caz în care, BitDefender se actualizează automat.

Dacă sunteți conectat la Internet pe bandă largă sau DSL, BitDefender se actualizează singur: Caută noi semnături de viruşi când deschideți calculatorul şi la fiecare **3 ore** apoi. Dacă noi semnături de viruşi sunt disponibile, BitDefender se va actualiza singur.

SFAT: Dacă vă conectați la Internet prin dial-up, este o idee bună să faceți un obicei din a actualiza BitDefender manual.

Actualizare manuală

În caz că nu ați deschis deja consola de administrare, o puteți accesa din meniul Windows Start, urmând calea **Start** → **Programs** → **BitDefender** → **BitDefender 8 Standard** sau mai rapid, faceți dublu-clic pe icoana BitDefender din bara de sistem.

În consola de administrare, faceți clic pe tab-ul **Actualizare**.

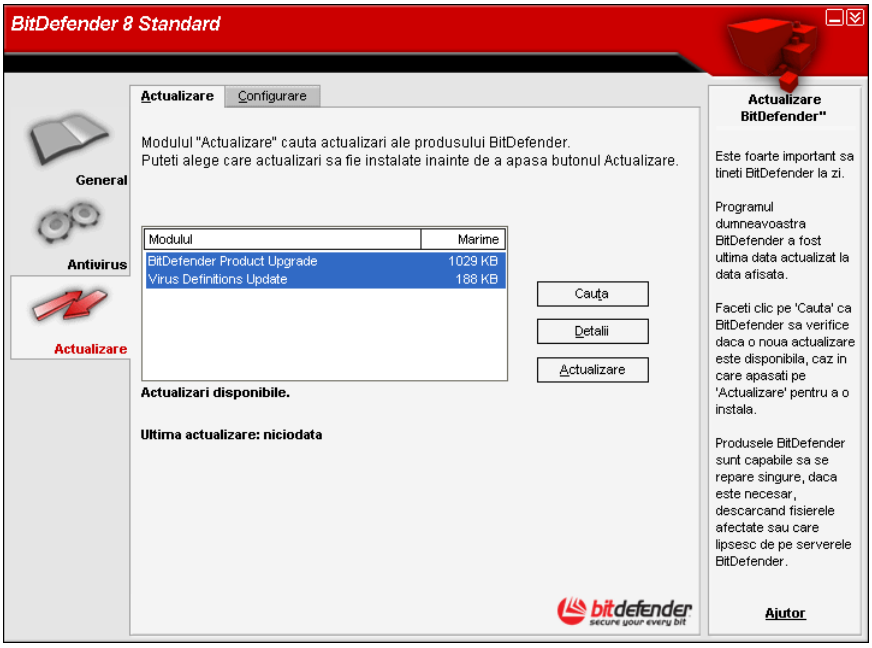


Figura 40

Actualizarea manuală se poate face oricând, chiar dacă produsul este setat să se actualizeze automat. Pentru a actualiza produsul manual, trebuie să urmați paşii:

➔ Faceți clic pe **Cauta**.

Modulul **Actualizare** se va conecta la serverul de actualizare al BitDefender şi va verifica dacă există actualizări disponibile.

➔ Dacă se găseşte o actualizare disponibilă, numele si dimensiunea acesteia vor fi afişate. Faceți clic pe **Actualizeaza** pentru a porni procesul de actualizare.

SFAT: Dacă doriți să vedeți ce fişiere vor fi actualizate, faceți clic pe **Detalii**.

➔ Dacă nu se găseşte nici o actualizare va apărea un mesaj.

Notă

La finalizarea procesului de actualizare poate fi necesară restartarea calculatorului. Vă recomandăm să o realizați cât mai repede posibil.

Actualizare automată

Dacă sunteți un utilizator avansat, faceți clic pe tab-ul **Setari** pentru a configura modulul **Actualizare**.

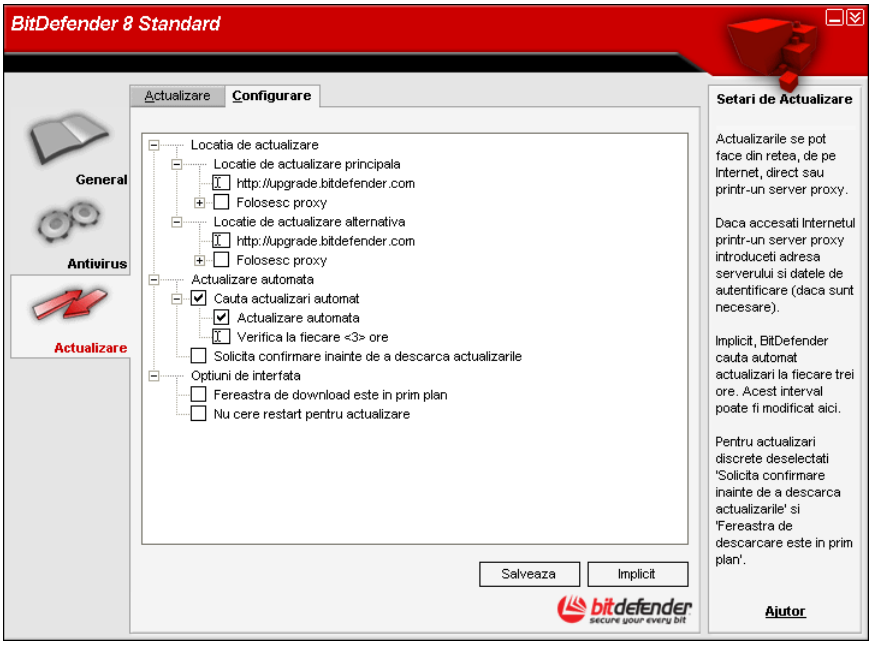


Figura 41

Actualizările pot fi realizate din rețeaua locală, de pe Internet, direct sau printr-un server proxy.

Fereastra de configurare a modulului Actualizare conține trei categorii de opțiuni (**Locatia de actualizare**, **Actualizare automata**, **Optiuni de interfata**) organizate într-un meniu expandabil, similar celor din Windows.

Faceți clic pe semnul “+” pentru a deschide o opțiune sau faceți clic pe “-” pentru a închide o opțiune.

Locația de actualizare

Pentru o actualizare mai sigură şi mai rapidă, puteți configura două locații de actualizare: o **Locație de actualizare principală** şi o **Locație de actualizare alternativă**. Pentru ambele este necesară configurarea următoarelor opțiuni.

➔ Dacă sunteți conectat la o rețea care plasează semnăturile de viruşi BitDefender local, aici puteți modifica locația de actualizare. Implicit aceasta este: http://upgrade.bitdefender.com.

➔ **Folosesc proxy** – În cazul în care compania foloseşte un server proxy selectați această opțiune. Următoarele informații trebuiesc specificate.

- **Proxy** – introduceți adresa IP sau numele serverului proxy precum şi portul pe care îl foloseşte BitDefender pentru a se conecta la serverul proxy.

  Sintaxă: `nume: port` sau `ip: port`.

- **Utilizator –** introduceți un nume de utilizator recunoscut de proxy.

Sintaxă: `domeniu\utilizator`.

- **Parolă –** introduceți o parolă validă pentru numele de utilizator introdus.

Actualizare automată

➔ **Cauta actualizari automat** – Această opțiune setează BitDefender să verifice automat serverele noastre în căutarea actualizărilor disponibile.

- **Actualizeaza automat** - Dacă BitDefender găseşte o nouă actualizare pe server, atunci, cu această opțiune activată, BitDefender descarcă şi instalează actualizarea.
- **Verifica la fiecare <3> ore** - Setează la cât timp BitDefender caută actualizări. Perioada setată implicit este de 3 ore.

➔ Păstrați opțiunea **Solicita confirmare inainte de a descarca actualizarile** pentru a fi întrebat înaintea descărcării şi instalării actualizărilor.

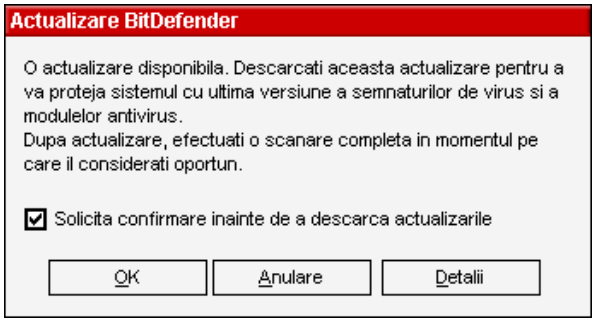


Figure 42

Faceți clic pe **OK** pentru a porni procesul de actualizare, faceți clic pe **Detalii** pentru a vedea ce fişiere vor fi actualizate sau faceți clic pe **Anulare** pentru a actualiza mai târziu.

Opțiuni interfață

➔ **Fereastra de download este in prim plan** – Implicit, actualizările produsului nu sunt realizate în prim plan. Dacă doriți ca actualizarea să fie realizată in prim plan, însemnând că fereastra care reprezintă grafic procesul de actualizare va apărea deasupra celorlalte ferestre, selectați această opțiune.

➔ **Nu cere restart pentru actualizare** - Dacă o actualizare necesită restartarea sistemului, produsul işi va continua funcționarea folosind fişierele vechi până când utilzatorul va reporni calculatorul din proprie inițiativă. Utilizatorului nu i se va cere repornirea calculatorului şi astfel actualizarea BitDefender nu va interfera cu activitatea utilizatorului.

Apăsați **Salveaza** pentru a salva modificările făcute. Dacă apăsați **Implicit** veți reveni la setările implicite.

Recomandări de utilizare

Antivirus

Paşi de urmat pentru a vă asigura un calculator fără viruşi:

1. După finalizarea procesului de instalare, vă recomandăm să înregistrați produsul, după cum este descris în secțiunea Înregistrare produs.
2. Realizați o actualizare manuală a semnăturilor de viruşi. În **Consola de Administrare BitDefender**, intrați în modulul **Actualizare** şi faceți clic pe **Cauta**.
3. Realizați o scanare completă a sistemului (după cum este descris în secțiunea scanare imediată a acestui ghid de utilizare).
4. În secțiunea Status a modulului **General**, păstrați activate cele mai importante caracteristici ale BitDefender: Scutul Antivirus şi Actualizarea automată.
5. Programați BitDefender să vă scaneze sistemul cel puțin o dată pe săptămână, folosind programul asistent din secțiunea Planificare.

   SFAT: Modulul Planificare vă permite să programați scanări complete ale sistemului în timpul în care nu folosiți calculatorul.

7

Întrebări frecvente

General

1. **Î:** Cum îmi dau seama dacă BitDefender funcționează?
   R: În modulul **General**, accesați secțiunea Status şi citiți statisticile.

2. **Î:** Care sunt cerințele de sistem?
   R: Puteți afla cerințele de sistem în secțiunea Instalare.

3. **Î:** Cum dezinstalez BitDefender?
   R: Urmați calea: **Start** → **Programs** → **BitDefender 8** → **Modificare, Reparare sau Dezinstalare** iar în fereastra care va apărea apăsați butonul **Dezinstalare**. Aceasta va porni procesul de dezinstalare.

4. **Î:** Unde introduc numărul serial (cheia de licență)?
   R: În modulul **General**, accesați secțiunea Inregistrare şi faceți clic pe butonul **Introduceti serie noua…**.

Antivirus

5. **Î:** Cum realizez o scanare completă a sistemului?
   R: În modulul **General**, accesați secțiunea Scanare, selectați opțiunea **Discuri locale** şi faceți clic pe butonul **Scaneaza**.

6. **Î:** Cât de des ar trebui să-mi scanez calculatorul?
   R: Vă recomandăm să vă scanați calculatorul cel puțin o dată pe săptămână.

7. **Î:** Cum pot să scanez automat fiecare fişier pe care îl transfer în calculator?
   R: BitDefender scanează toate fişierele accesate. Tot ce trebuie să faceți este să păstrați Scutul Antivirus activat.

8. **Î:** Cum programez BitDefender să îmi scaneze calculatorul periodic?
   R: În modulul **General**, accesați secțiunea Planificare, faceți clic pe **Adauga** şi urmați paşii programului asistent.

9. **Î:** Ce se întâmplă cu fişierele din zona de carantină?
   R: Puteți trimite aceste fişiere la Laboratorul BitDefender pentru analiză, dar înainte trebuie să specificați setările de e-mail (accesați secțiunea Carantina şi faceți clic pe **Setari**).

Actualizare

10. **Î:** De ce este necesar să actualizez BitDefender?
R: De fiecare dată când realizați o actualizare noi semnături de viruşi vor fi adăugate la motoarele Antivirus şi noi reguli vor fi adăugate filtrelor euristic şi URL.

11. **Î:** Cum actualizez BitDefender?
R: Implicit, BitDefender se actualizează automat la fiecare 3 ore. Dar puteți realiza şi actualizări automate sau modifica intervalul de timp pentru actualizarea automată în modulul Actualizare.

8

Vocabular

ActiveX	ActiveX este un mod de scriere a programelor astfel încât să poată fi apelate de celelalte programe şi sisteme de operare. Tehnologia ActiveX este utilizată pentru realizarea de pagini Web interactive care se comportă ca nişte aplicaţii şi nu ca nişte simple pagini statice. Cu elemente de ActiveX, utilizatorii pot răspunde la întrebări, să utilizeze butoane şi să interacţioneze şi în alte moduri cu pagina Web. Controalele ActiveX sunt adesea scrise utilizând limbajul Visual Basic.
Actualizare	Reprezintă o versiune nouă de produs hardware sau software proiectat să înlocuiască o versiune mai veche a aceluiaşi produs. În afară de acesta, rutinele de instalare verifică dacă există instalată pe calculatorul dumneavoastră o altă versiune mai veche; dacă nu, nu puteţi instala actualizarea. BitDefender dispune de modulul său propriu care realizează actualizarea automatică sau manuală.
Applet-uri Java	Reprezintă un program Java care este proiectat să ruleze doar pe pagini web. Pentru a utiliza un applet pe o pagină web, trebuie specificate numele applet-ului şi mărimea acestuia. Când este accesată o pagină web, browser-ul descarcă applet-ul de pe un server şi îl rulează pe maşina utilizatorului (clientul). Applet-urile diferă de aplicaţii prin aceea că sunt guvernate de un protocol de securitate strict. Astfel, că deşi pot rula pe calculatorul unui utilizator, ele nu pot citi sau scrie date pe aceste calculatoare. Applet-urile sunt restricţionate de domeniul de care aparţin în ceea ce priveşte scrierea şi citirea datelor.
Arhivă	Un fişier care conţine unul sau mai multe fişiere într-un format comprimat.
Backdoor	Reprezintă o gaură de securitate realizată în mod deliberat. Motivaţia acestor "găuri" nu este întotdeauna malitioasă: unele sisteme de operare, de exemplu, sunt puse în circulaţie cu conturi privilegiate pentru tehnicienii din service sau de responsabilii cu mentenanţă produsului din partea vânzătorului.
Browser	Este prescurtarea de la *Web Browser*, o aplicaţie utilizată pentru a localiza şi încărca pagini de Web. Două din cele mai populare browsere sunt Netscape Navigator şi Microsoft Internet Explorer. Ambele sunt browsere grafice, ceea ce înseamnă că pot afişa atât grafice cât şi text. În plus, cele mai moderne browsere pot prezenta informaţii multimedia, incluzând sunet şi animaţie.

Cale	1.Reprezintă direcția exactă către un fişier de pe un calculator. Aceasta direcție este specificată utilizând sistemul ierarhic de organizare a fişierelor de sus în jos, specificând drive-ul, directorul, subdirectoarele, numele fişierului şi extensia acestuia, ca de exemplu: c:jobscompany/resume.txt. 2.Ruta între două puncte, cum ar fi de exemplu canalul de comunicație între două computere.
Client de mail	Un client de mail este o aplicație care vă permite să trimiteți şi să recepționați mesaje.
Cookie	Un cookie reprezintă un set de date pe care un server Web îl transmite către un browser atunci când utilizatorul vizitează prima oară site-ul şi care este actualizat de fiecare dată când utilizatorul accesează din nou site-ul. Server-ul, la fel ca şi browser-ul, salvează informațiile despre utilizator conținute în cookie. Aceste informații sunt stocate sub forma unui fişier text în directoarele de sistem ale browser-elor Netscape şi Explorer. Nu toate browser-ele suportă cookie. Fişierele cookie stochează informații cum ar fi numele utilizatorului şi parola, cât şi ce părți din site au fost vizitate. Browser-ul împarte fiecare cookie doar cu server-ul care l-a generat, celelalte servere le pot citi doar pe cele generate de ele. Unele fişiere cookie sunt programate cu dată de expirare, astfel încât ele vor fi şterse automat după o anumită perioadă de timp.
Download	Reprezintă copierea (de obicei a unui întreg fişier) de pe o sursă pricipală pe un dispozitiv periferic. Termenul este adesea utilizat pentru a descrie procesul de copiere a unui fişier de pe un serviciu on-line pe calculatorul unui utilizator. De asemenea se mai poate referi şi la copierea unui fişier de pe un server de rețea pe un calculator din rețea.
Drive de disc	Este un dispozitiv care citeşte date de pe un disc şi scrie date pe un disc. Un **drive de hard** disc citeşte / scrie date de pe / pe hard disc. Un **drive de floppy** accesează dischetele floppy. Drive-ele de disc pot fi sau *interne* (incorporate în interiorul unui calculator) sau *externe* (plasate într-o locație separată care este conectată la calculator).
E-mail	Se referă la poşta electronică. Acesta este un serviciu care transmite mesaje prin intermediul rețelei locale sau globale.
Elemente din startup	Orice fişier plasat în acest director se va deschide de fiecare dată când calculatorul este pornit. De exemplu, un sunet care se va auzi atunci când este pornit calculatorul sau chiar aplicații sunt considerate elemente de startup. În mod normal, un alias al programului este plasat în acest director, şi nu direct fişierul.
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. Modulul Planificare este un instrument care vă ajută să programați evenimente de scanare.
Extensie de fişier	Reprezintă porțiunea dintr-un nume de fişier ce urmează după caracterul punct, şi care indică tipul de date pe care le stochează fişierul. De obicei aceasta este formată din una până la trei caractere. De exemplu: "txt" pentru fişierele text oarecare, "c" pentru fişierele sursă scrise în limbajul C, etc.

Fals pozitiv	Apare atunci când un produs de scanare antivirus detectează un fişier ca fiind infectat când de fapt acesta nu este infectat.
Fişier de raport	Reprezintă un fişier care listează acțiunile care au avut loc. De exemplu, BitDefender menține un fişier log (jurnal) în care sunt listate obiectele care au fost scanate, numele fişierelor, numărul de arhive şi fişiere scanate, câte fişiere infectate şi suspecte au fost găsite.
IP	Un protocol rutabil din suita protocoalelor **TCP / IP** căruia i se atribuie adresarea IP, rutarea, fragmentarea cât şi reasamblarea pachetelor IP.
Linie de comandă	Într-o interfață linie de comandă, utilizatorul scrie comenzile în spațiul prevăzut direct pe ecran utilizând limbajul de comandă.
Memorie	Reprezintă arii de stocare a datelor din interiorul computerului. Fiecare calculator dispune de o anumită capacitate de memorie fizică, referită de obicei prin memorie principală sau RAM.
Metoda euristică	Reprezintă o metodă bazată pe anumite reguli pentru identificarea de viruşi noi. Această metodă de scanare nu se bazează pe semnături de viruşi cunoscuți. Avantajul metodei euristice e dat de faptul că nu poate fi păcălită de o nouă variantă a unui virus deja existent. Totuşi ocazional poate raporta un cod suspicios în programe normale, generând aşa-numitul "fals pozitiv".
Metoda non-euristică	Această metodă de scanare se bazează pe semnături specifice de viruşi. Avantajul metodelor ne-euristice constă în aceea că scannerul nu poate fi "păcălit" de ceea ce poate părea un virus şi din acest motiv nu generează fals pozitiv.
Port	(1) Reprezintă o interfață a unui calculator la care se poate conecta un dispozitiv. Calculatoarele personale dispun de diferite tipuri de porturi. De exemplu, există porturi externe pentru conectarea modemului, imprimantei, mouse-ului, şi a altor dispozitive periferice. (2) În rețelele TCP / IP şi UDP acestea reprezintă un punct terminus al unei conexiuni logice. Numărul portului identifică ce tip de port este. De exemplu, portul 80 este utilizat pentru traficul HTTP.
Programe împachetate	Reprezintă un fişier în format comprimat. Multe din sistemele de operare şi aplicații conțin comenzi care vă dau posibilitatea de a împacheta un fişier astfel încât să ocupe mai putină memorie. De exemplu, să presupunem că aveți un fişier text care conține zece caractere reprezentând spații. În mod normal, acesta ar necesita zece biți de memorie pentru a fi stocați. Programul care realizează împachetarea 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.
Script	Un alt termen pentru fişiere macro sau de tip "bat", un script reprezintă o listă de comenzi care pot fi executate fără intervenția utilizatorului.
Sector de boot	Un sector la începutul fiecărui disc care identifică arhitectura discului (mărimea sectorului, mărimea clusterului şi altele). În cazul discurilor de startup, sectorul de boot conține un program care încarcă sistemul de operare.

Semnătura unui virus	Reprezintă tiparul binar al unui virus, utilizat de un program antivirus pentru detecția şi eliminarea virusului.
Bara de sistem (system tray)	Acest concept a fost introdus odată cu apariția sistemului Windows 95. Acesta este plasat în taskbar-ul de Windows (situat lângă ceas) şi conține iconițe pentru accesul rapid la aplicații sistem cum ar fi cele legate de fax, imprimantă, modem, volum, şi altele. Executați dublu-clic cu mouse-ul pe o iconiță pentru a vizualiza şi accesa elementele.
TCP/IP	**Transmission Control Protocol** / **Internet Protocol** - Un set de protocoale de rețea folosite în mod larg în domeniul Internet şi care asigură comunicarea între rețelele de calculatoare interconectate având arhitecturi hardware şi sisteme de operare diferite. TCP/IP include standarde referitoare la realizarea comunicării între calculatoare cât şi convenții folosite în conectarea rețelelor şi rutării traficului.
Troian	Este un program distructiv care este mascat sub forma unei aplicații benigne. Spre deosebire de viruşi, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cei mai mascați troieni este acela care pretinde că elimină viruşii de pe computerul dumneavoastră, dar în loc de aceasta, introduce viruşi pe calculatorul dumneavoastră. Termenul provine de la o poveste din opera "Iliada" lui Homer, în care grecii oferă duşmanilor lor, troienii, în semn de pace un cal gigantic de lemn. Dar după ce troienii aduc acest cal în interiorul oraşului lor, din interiorul calului ies o mulțime de soldați greci, care deschid porțile cetății, permițându-le celorlalți soldați greci să pătrundă în oraş şi să captureze Troia.
Vierme (worm)	Reprezintă un program care se autopropagă în interiorul unei rețele, reproducându-se pe măsură ce se răspândeşte. Nu se poate ataşa la alte programe.
Virus	Reprezintă un program sau o bucată de cod care se încarcă pe calculator fără ştirea dumneavoastră şi rulează independent de voința dumneavoastră. Cea mai mare parte a viruşilor se pot şi înmulți. Toți viruşii informatici sunt creați de om. Un simplu virus care poate realiza copii ale sale este relativ simplu de reprodus. Chiar şi un asemenea virus este periculos întrucât poate duce la blocarea sistemului, prin utilizarea la maximum a resurselor de memorie. Un virus şi mai periculos este acela care este capabil să se răspândească în rețea şi poate să treacă de sistemele de securitate.
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.
Virus de macro	Un tip de virus informatic este acela inclus ca macro într-un document. Multe aplicații cum ar fi de exemplu Microsoft Word şi Excel suportă limbaje macro puternice. Aceste limbaje permit încapsularea de macro-uri în documente şi execută aceste macro-uri de fiecare dată când este deschis documentul.
Virus polimorf	Reprezintă un virus care îşi schimbă forma cu fiecare fişier pe care îl infectează. Din cauză că nu au un tipar binar consistent, asemenea viruşi sunt greu de identificat.

9

Informații de contact

Ca orice companie orientată spre satisfacerea cerințelor clienților săi, Softwin asigură clienților suport tehnic rapid şi eficient. Centrul de suport tehnic este permanent la curent cu ultimele apariții şi descrieri de viruşi şi este gata oricând să vă răspundă la eventualele nelămuriri şi probleme pe care le aveți astfel încât să obțineți în timp util informațiile necesare.

SOFTWIN apreciază toate sugestiile şi idei din partea dumneavoastră privind îmbunătățirea produsului şi a calității serviciilor noastre. De asemenea, dacă aveți informații referitoare la noi viruşi aşteptăm descrierile dumneavoastră. Vă rugăm să nu ezitați să ne contactați.

Departamentul clienți: sales@bitdefender.ro

Asistență tehnică: suport@bitdefender.ro.

Telefon: 0040-21-233 07 80

Web site produs: www.bitdefender.ro.

Adresă:

SOFTWIN
Str. Fabrica de Glucoză, Nr.5
Bucureşti, Sector 2, CP 52-93
ROMÂNIA

Puteți trimite observații despre acest document la adresa: documentation@bitdefender.com