bitdefender® 9

Professional Plus

User's guide

- Antivirus
- Antispam
- Firewall
- Antispyware

BitDefender 9 Professional Plus
User's guide

SOFTWIN

Published 2006.05.19
Version 9.5

Legal Notice

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of SOFTWIN, and SOFTWIN is not responsible for the content of any linked site. If you access a third-party website mentioned in this guide, you will do so at your own risk. SOFTWIN provides these links only as a convenience, and the inclusion of the link does not imply that SOFTWIN endorses or accepts any responsibility for the content of those third-party sites.

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners.

Table of Contents

License and Warranty

This License Agreement is a legal agreement between you (either an individual or a single entity end user) and SOFTWIN for use of the SOFTWIN software product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("BitDefender"), all of which are protected by U.S. and international copyright laws and international treaty protection. By installing, copying, or otherwise using BitDefender, you agree to be bound by the terms of this agreement. If you do not agree to the terms of this agreement, do not install or use BitDefender; you may, however, return it to your place of purchase for a full refund within 30 days after your purchase. Verification of your purchase may be required.

BitDefender is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. BitDefender is licensed, not sold.

GRANT OF LICENSE. SOFTWIN hereby grants you and only you the following non-exclusive license to use BitDefender:

APPLICATION SOFTWARE. You may install and use one copy of BitDefender, or any prior version for the same operating system, on a single computer terminal. The primary user of the computer on which BitDefender is installed may make one additional (i.e. second) copy for his or her exclusive use on a portable computer.

NETWORK USE. You may also store or install a copy of BitDefender on a storage device, such as a network server, used only to install or run the BitDefender on your other computers over an internal network; however, you must purchase and dedicate a separate license for each separate computer terminal on which BitDefender is installed or run from the storage device. A license for BitDefender may not be shared or used concurrently on different computers or computer terminals. You should purchase a license pack if you require multiple licenses for use on multiple computers or computer terminals.

LICENSE PACKS. If you purchase a License Pack and you have acquired this License Agreement for multiple licenses of BitDefender, you may make the number of additional copies of the computer software portion of BitDefender specified above as "Licensed copies". You are also entitled to make a corresponding number of secondary copies for portable computer use as specified above in the section entitled "Application Software".

TERM OF LICENSE. The license granted hereunder shall commence on the date that you install, copy or otherwise first use BitDefender and shall continue only on the computer on which it is initially installed.

UPGRADES. If BitDefender is labeled as an upgrade, you must be properly licensed to use a product identified by SOFTWIN as being eligible for the upgrade in order to use the BitDefender. A BitDefender labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this License Agreement. If BitDefender is an upgrade of a component of a package of software programs that you licensed as a single product, BitDefender may be used and transferred only as part of that single product package and may not be separated for use on more than one computer.

COPYRIGHT. All right, title and interest in and to BitDefender and all copyright rights in and to BitDefender (including but not limited to any images, photographs, logos, animations, video, audio, music, text, and "applets" incorporated into BitDefender), the accompanying printed materials, and any copies of BitDefender are owned by SOFTWIN. BitDefender is protected by copyright laws and international treaty provisions. Therefore, you must treat BitDefender like any other copyrighted material except that you may install BitDefender on a single computer provided you keep the original solely for backup or archival purposes. You may not copy the printed materials accompanying BitDefender. You must produce and include all copyright notices in their original form for all copies created irrespective of the media or form in which BitDefender exists. You may not sub-license, rent, sell, or lease BitDefender. You may not reverse engineer, recompile, disassemble, create derivative works, modify, translate, or make any attempt to discover the source code for BitDefender.

LIMITED WARRANTY. SOFTWIN warrants that the media on which BitDefender is distributed is free from defects for a period of thirty days from the date of delivery of BitDefender to you. Your sole remedy for a breach of this warranty will be that SOFTWIN, at its option, may replace the defective media upon receipt of the damaged media, or refund the money you paid for BitDefender. SOFTWIN does not warrant that BitDefender will be uninterrupted or error free or that the errors will be corrected. SOFTWIN does not warrant that BitDefender will meet your requirements. SOFTWIN HEREBY DISCLAIMS ALL OTHER WARRANTIES FOR BITDEFENDER, WHETHER EXPRESSED OR IMPLIED. THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESSED OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON INFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

DISCLAIMER OF DAMAGES. Anyone using, testing, or evaluating BitDefender bears all risk to the quality and performance of BitDefender. In no event shall SOFTWIN be liable for any damages of any kind, including, without limitation, direct or indirect damages arising out of the use, performance, or delivery of BitDefender, even if SOFTWIN has been advised of the existence or possibility of such damages. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL

DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN NO CASE SHALL SOFTWIN'S LIABILITY EXCEED THE PURCHASE PRICE PAID BY YOU FOR BITDEFENDER. The disclaimers and limitations set forth above will apply regardless of whether you accept or use, evaluate, or test BitDefender.

IMPORTANT NOTICE TO USERS. THIS SOFTWARE IS NOT FAULT-TOLERANT AND IS NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. THIS SOFTWARE IS NOT FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, OR COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY OR PROPERTY DAMAGE.

GOVERNMENT RESTRICTED RIGHTS/RESTRICTED RIGHTS LEGEND. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of Commercial Computer Software-Restricted Rights clause at 48 CFR 52.227-19, as applicable. Contact SOFTWIN, at 5, F-ca de Glucoza str., 72322-Sect.2, Bucharest, Romania, or at Tel No: 40-21-2330780 or Fax:40-21-2330763.

GENERAL. This Agreement will be governed by the laws of Romania and by the international copyright regulations and treaties. This Agreement may only be modified by a license addendum, which accompanies this Agreement or by a written document which has been signed, by both you and SOFTWIN. This Agreement has been written in the English language only and is not to be translated or interpreted in any other language. Prices, costs and fees for use of BitDefender are subject to change without prior notice to you. In the event of invalidity of any provision of this Agreement, the invalidity shall not affect the validity of the remaining portions of this Agreement. BitDefender and BitDefender logos are trademarks of SOFTWIN. Microsoft, Windows, Excel, Word, the Windows logo, Windows NT, Windows 2000 are registered trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners.

Preface

This guide is intended to all users who have chosen **BitDefender 9 Professional Plus** as a security solution for their personal computers. The information presented in this book is suitable not only for computer literates, it is accessible to everyone who is able to work under Windows.

This book will describe for you **BitDefender 9 Professional Plus**, the Company and the team who built it, will guide you through the installation process, will teach you how to configure it. You will find out how to use **BitDefender 9 Professional Plus**, how to update, test and customize it. You will learn how to get best from BitDefender.

We wish you a pleasant and useful lecture.

1. Conventions used in this book

1.1. Typographical conventions

Several text styles are used in the book for an improved readability. Their aspect and meaning are presented in the table below.

Appearance	Description
`sample syntax`	Syntax samples are printed with `monospaced` characters.
http://www.bitdefender.com	The URL link is pointing to some external location, on http or ftp servers.
<`support@bitdefender.com`>	E-mail messages are inserted in the text for contact information.
"Preface" (p. xiii)	This is an internal link, towards some location inside the document.
`filename`	File and directories are printed using `monospaced` font.
option	All the product options are printed using **strong** characters.

Appearance	Description
`sample code listing`	The code listing is printed with `monospaced` characters.

1.2. Admonitions

The admonitions are in-text notes, graphically marked, bringing to your attention additional information related to the current paragraph.

Note

The note is just a short observation. Although you can omit it, the notes can provide valuable information, such as specific feature or a link to some related topic.

Important

This requires your attention and is not recommended to skip over it. Usually, it provides non-critical but significant information.

Warning

This is critical information you should treat with increased caution. Nothing bad will happen if you follow the indications. You should read and understand it, because it describes something extremely risky.

2. The book structure

The book consists of six parts, containing the major topics: Product installation, Description and features, Management Console, Best practices, BitDefender Rescue CD and Getting help. Moreover, a glossary is provided to clarify some technical terms.

Product installation. Step by step instructions for installing BitDefender on a workstation. This is a comprehensive tutorial on installing **BitDefender 9 Professional Plus**. Starting with the prerequisites for a successfully installation, you are guided through the whole installation process. Finally, the removing procedure is described in case you need to uninstall BitDefender.

Description and features. A short introduction to BitDefender. It explains who BitDefender is, who SOFTWIN and Data Security Division are. **BitDefender 9 Professional Plus**, its features and the product modules are presented to you.

Management console. Description of basic administration and maintenance of BitDefender. The chapters explain in detail all options of **BitDefender 9 Professional Plus**, how to register the product, how to scan your computer, how to configure the Antispam module, how to configure the Firewall module and how to perform the updates.

Best practices. Follow the steps described in here in order to ensure a computer free from viruses&spam&spyware.

BitDefender Rescue CD. Description of the BitDefender Rescue CD. It helps understand and use the features offered by this bootable CD.

Getting help. Where to look and where to ask for help if something unexpected appears. It includes a FAQ section too.

Glossary. The Glossary tries to explain some technical and uncommon terms you will find in the pages of this document.

3. Request for Comments

We invite you to help us improve the book. We have tested and verified all of the information to the best of our ability. Please write to tell us about any flaws you find in this book or how you think it could be improved, to help us provide you with the best documentation possible.

Let us know by sending an e-mail to <documentation@bitdefender.com>.

Product installation

1. BitDefender 9 Professional Plus installation

The **BitDefender 9 Professional Plus installation** section of this user guide contains the following topics:

- System requirements
- Installation steps
- Upgrade
- Removing, repairing or modifying BitDefender features

1.1. System requirements

To ensure a proper functioning of the product, before installation, verify that the following system requirements are met:

- **Minimum Processor** - Pentium MMX 200 MHz
- **Minimum hard disk space** - 40MB
- **Minimum RAM Memory** - 64MB (128MB Recommended)
- **Operating system** - Windows 98/NT-SP6/ME/2000/XP; Internet Explorer 5.5 (+)

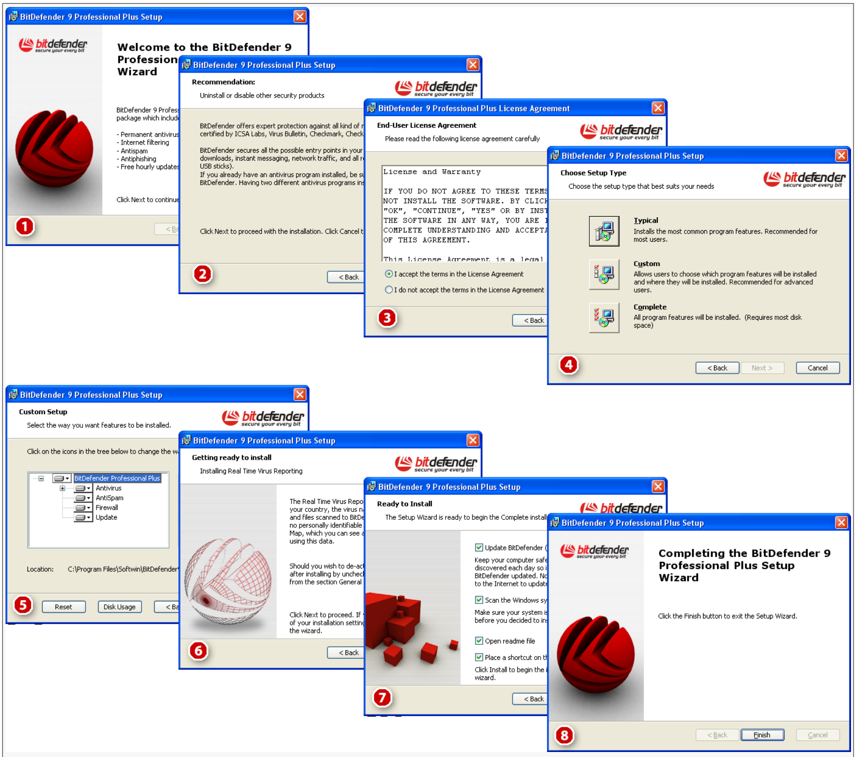
Warning

BitDefender 9 Professional Plus can not be installed on Windows NT 4.0 Server, Windows 2000 Server or Windows 2003 Server. For these platforms we recommend the corporate products for file servers, gateways and mail servers.

1.2. Installation steps

Locate the setup file and double-click it. This will launch a wizard, which will guide you through the setup process:

Installation steps:



BitDefender 9 Professional Plus Setup

Welcome to the BitDefender 9
Profession
Wizard

BitDefender 9 Profes
package which includ

- Permanent antivirus
- Internet filtering
- Antispam
- Antiphishing
- Free hourly update

Click Next to continue

BitDefender 9 Professional Plus Setup

Recommendation:
Uninstall or disable other security products

BitDefender offers expert protection against all kind of
certified by ICSA Labs, Virus Bulletin, Checkmark, Check

BitDefender secures all the possible entry points in your
downloads, instant messaging, network traffic, and all r
USB sticks).
If you already have an antivirus program installed, be su
BitDefender. Having two different antivirus programs in

Click Next to proceed with the installation. Click Cancel t

BitDefender 9 Professional Plus License Agreement

End-User License Agreement
Please read the following license agreement carefully

```
License and Warranty

IF YOU DO NOT AGREE TO THESE TERMS
NOT INSTALL THE SOFTWARE. BY CLICK
"OK", "CONTINUE", "YES" OR BY INST
THE SOFTWARE IN ANY WAY, YOU ARE I
COMPLETE UNDERSTANDING AND ACCEPTA
OF THIS AGREEMENT.

This License Agreement is a legal
```

● I accept the terms in the License Agreement
○ I do not accept the terms in the License Agreement

BitDefender 9 Professional Plus Setup

Choose Setup Type
Choose the setup type that best suits your needs

Typical
Installs the most common program features. Recommended for most users.

Custom
Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.

Complete
All program features will be installed. (Requires most disk space)

BitDefender 9 Professional Plus Setup

Custom Setup
Select the way you want features to be installed.

Click on the icons in the tree below to change the w

BitDefender Professional Plus
Antivirus
AntiSpam
Firewall
Update

Location: C:\Program Files\Softwin\BitDefender

BitDefender 9 Professional Plus Setup

Getting ready to install
Installing Real Time Virus Reporting

The Real Time Virus Repo
your country, the virus n
and files scanned to BitDe
no personally identifiable
Map, which you can see a
using this data.

Should you wish to de-act
after installing by unchec
from the section General

Click Next to proceed. If
of your installation setting
the wizard.

BitDefender 9 Professional Plus Setup

Ready to Install
The Setup Wizard is ready to begin the Complete install

☑ Update BitDefender (
Keep your computer safe
discovered each day so i
BitDefender updated. No
to the Internet to update

☑ Scan the Windows sy
Make sure your system is
before you decided to in

☑ Open readme file

☑ Place a shortcut on th

Click Install to begin the i
wizard.

BitDefender 9 Professional Plus Setup

Completing the BitDefender 9
Professional Plus Setup
Wizard

Click the Finish button to exit the Setup Wizard.

Installation steps

1. Click **Next** to continue or click **Cancel** if you want to quit installation.

2. Click **Next** to continue or click **Back** to return to the first step.

3. Please read the License Agreement, select **I accept the terms in the License Agreement** and click **Next**. If you do not agree with these terms click **Cancel**. The installation process will be abandoned and you will exit setup.

4. You can choose what kind of installation you want: typical, custom or complete.

   - **Typical** - The program will be installed with the most common options. This is the recommended option for most users.

- **Custom** - You may choose the components you want to install. Recommended for advanced users only.
- **Complete** - For full installation of the product. All BitDefender modules will be installed.

  If you select **Typical** or **Complete** you will skip step 5.

5. If you have selected **Custom**, a new window will appear containing all the BitDefender components listed so that you may select the ones you would like to install.

   If you click any component name, a short description (including the minimum space required on the hard disk) will appear on the right side. If you click any component icon a window will appear where you can choose to install or not the selected module.

   You can select the folder where you want to install the product. The default folder is `C:\Program Files\Softwin\BitDefender 9`.

   If you want to select another folder, click **Browse** and in the window that will open, select the folder you wish BitDefender to be installed in. Click **Next**.

6. Click **Next**.

7. You have four options selected by default:

   - **Update BitDefender** - to update BitDefender at the end of the installation. Your system must be connected to the Internet to update.
   - **Scan the Windows system folder** - to scan the Windows system folder at the end of the installation.
   - **Open readme file** - to open the readme file at the end of the installation.
   - **Place a shortcut on the desktop** - to place a shortcut to BitDefender on your desktop at the end of the installation.

   Click **Install** in order to begin the installation of the product.

8. Click **Finish** to complete the product installation. If you have accepted the default settings for the installation path, a new folder named `Softwin` is created in `Program Files` and it contains the subfolder `BitDefender 9`.

   Note

   You may be asked to restart your system so that the setup wizard can complete the installation process.

1.3. Upgrade

The upgrade procedure can be done in one of the following ways:

- Install without removing the previous version - v8 to v9 only

  Double-click the setup file and follow the wizard described in the "*Installation steps*" (p. 19) section.

  Important
  During the installation process an error message caused by the `Filespy service`, will appear. Click **OK** to continue the installation.

- Uninstall your previous version and install the new one - for all BitDefender versions

  First of all you have to remove your previously version, restart the computer and install the new one as described in the "*Installation steps*" (p. 19) section.

Important
If you upgrade from v8 to v9 we recommend you to save the BitDefender settings. If you upgrade from v8 to v9 we recommend you to save the BitDefender settings, the Friends list, the Spammers list and the Firewall rules. . After the upgrading process is over you may load them.

1.4. Removing, repairing or modifying BitDefender features

If you want to modify, repair or remove **BitDefender 9 Professional Plus**, follow the path from the Windows start menu: **Start** -> **Programs** -> **BitDefender 9** -> **Modify, Repair or Uninstall**.

You will be requested to confirm your choice by clicking **Next**. A new window will appear where you can select:

- **Modify** - to select new program components to add or to select currently installed components to remove;

- **Repair** - to re-install all program components installed by the previous setup;

  Important
  Before repairing the product we recommend you to save the Friends list, the Spammers list and the Firewall rules. You can also save the BitDefender settings and the Bayesian database. After the repairing process is over you may load them.

- **Remove** - to remove all installed components.

To continue setup, select one of the three options listed above. We recommend that you choose **Remove** for a clean re-installation. After the uninstall process is over, we recommend that you delete the `Softwin` folder from the `Program Files`.

Description and features

2. Overview

BitDefender provides security solutions to satisfy the protection requirements of today's computing environment, delivering effective threat management for over 41 million home and corporate users in more than 100 countries.

Designed to provide full protection for corporate network and systems, the BitDefender solution range comprises, beside antivirus protection, antispam, personal firewall and security management solutions. BitDefender also specializes in providing assistance with designing and establishing content security policies for corporate networks.

BitDefender Professional was the third product of its kind in the world to receive ICSA certification for Windows XP and the first to be awarded for groundbreaking innovation by the European Commission and Academies. BitDefender Antivirus is certified by all the major reviewers in the antivirus field - ICSA Labs, CheckMark, CheckVir, TÜV and Virus Bulletin.

BitDefender is headquartered in Bucharest, Romania and has offices in Tettnang, Germany, Barcelona, Spain and Florida, US. Website: http://www.bitdefender.com

2.1. Why BitDefender?

Proven. Most reactive antivirus producer. BitDefender fast reactivity in case of computer virus epidemic was confirmed beginning with the last outbreaks of CodeRed, Nimda and Sircam, as well as Badtrans.B or other dangerous, fast-spreading malicious codes. BitDefender was the first to provide antidotes against these codes and to make them freely available on the Internet for all affected people. Now, with the continuous expansion of the Klez virus - in various versions immediate antivirus protection has become once more a critical need for any computer system.

Innovative. Awarded for innovation by the European Commission and EuroCase. BitDefender has been proclaimed a winner of the European IST-Prize, awarded by the European Commission and by representatives of 18 academies in Europe. Now in its eighth year, the European IST Prize is a reward for groundbreaking products that represent the best of European innovation in information technology.

Comprehensive. Covers every single point of your network, providing complete security. BitDefender security solutions for the corporate environment satisfy the protection requirements of today's business environment, enabling management of all complex threats that endanger a network, from a small local area to large multi-server, multi-platform WAN's.

Your Ultimate Protection. The final frontier for any possible threat to your computer system. As virus detection based on code analysis has not always offered good results, BitDefender has implemented behavior based protection, providing security against newborn malware.

These are **the costs** that organizations want to avoid and what the security products are designed to prevent:

- Worm attacks
- Communication loss because of infected e-mails
- E-mail breakdown
- Cleaning and recovering systems
- Lost productivity experienced by end users because systems are not available
- Hacking and unauthorized access that causes damage

Some simultaneously **developments and benefits** can be accomplished by using the BitDefender security suite:

- Increase network availability by stopping the spread of malicious code attacks (i.e., Nimda, Trojan horses, DDoS).
- Protect remote users from attacks.
- Reduce administrative costs and deploys rapidly with BitDefender Enterprise management capabilities.
- Stop the spreading of malware through e-mail, using a BitDefender e-mail protection at the company's gateway.Temporarily or permanently block unauthorized, vulnerable, and expensive application connections.

2.2. Data Security Division

Ever since the beginning, SOFTWIN's Data Security Division approached data protection in a specific manner, with the first intelligent update, requiring no user intervention, the first remote antivirus management through WAP technology or the first Personal Firewall to be integrated within an antivirus engine to provide complete response to today's complex security threats.

Born to provide full data security at all critical levels in today's business environment, Data Security Division aims to ensure systems protection against computer viruses, to do antivirus research, to develop new technologies for monitoring all possible ways to infect a system and, last but not least, to educate the IT&C public on the danger of computer viruses.

BitDefender security solutions satisfy the protection requirements of today's business environment, enabling management of all complex threats that endanger a network, from a small local area to large multi-server, multi-platform WAN's.

2.3. SOFTWIN

Bucharest-based SOFTWIN is the leading provider of complex software solutions and services in Romania.

SOFTWIN focuses on providing software solutions and services that enable fast growing companies to solve critical business challenges and to capitalize on new business opportunities.

SOFTWIN enables companies to focus on their core business and expand to new markets, by outsourcing non-core activities.

SOFTWIN employs over 500 highly qualified professionals experienced in developing customized solutions and services.

Since its establishment in 1990, SOFTWIN's average annual revenue has increased by +30%.

SOFTWIN has 4 divisions, which also define the company's main business lines:

- CRM
- Business Information Solutions
- eContent Solutions
- Data Security Solutions

SOFTWIN provides services and solutions to customers worldwide. Over 90% of the company's turnover is achieved from exports to the US and European Union.

Using cutting edge technologies, SOFTWIN successfully developed over 500 software development projects, over 3,500 content structuring projects for international partners, having over 43 million data security solutions users in 80 countries worldwide and more than 1,500,000 client calls handled annually for CRM services.

3. BitDefender 9 Professional Plus

BitDefender 9 Professional Plus integrates antivirus, antispam and firewall modules into one comprehensive security package, tailored to meet the needs of computer users worldwide.

3.1. Antivirus

The mission of the Antivirus module is to ensure detection and removal of all viruses in the wild. BitDefender Antivirus uses robust scan engines, certified by ICSA Labs, Virus Bulletin, Checkmark, CheckVir and TÜV.

Behavioral Heuristic Analyzer in Virtual Environments. Behavioral Heuristic Analyzer in Virtual Environments (B-HAVE) emulates a virtual computer-inside-a-computer where pieces of software are run in order to check for potential malware behavior. This BitDefender proprietary technology represents a new security layer that keeps the operating system safe from unknown viruses by detecting malicious pieces of code for which signatures have not been released yet.

Permanent Antivirus&Antispyware Protection. The new and improved BitDefender scanning engines will scan and disinfect infected files on access, minimizing data loss. Infected documents can now be recovered, instead of being deleted.

Peer-2-Peer Applications Protection. Filters against viruses that spread via instant messaging and file sharing software applications.

Spyware scanning and cleaning. BitDefender can scan your system, or part of it, for known spyware threats. The scan uses a constantly updated spyware signature database.

Full E-mail Protection. BitDefender runs on the POP3/SMTP protocol level, filtering incoming and outgoing e-mail messages, regardless of the e-mail client used (MS Exchange, MS Outlook, MS Outlook Express, Netscape, Eudora, Pegasus, The Bat, etc.), without any additional configuration.

3.2. Antispam

Quite simply put, the BitDefender Antispam module deals with the problem of spam, so you don't have to.

Anti-Phishing. Stay clear of malicious e-mail messages trying to trick you into giving away your bank account info with BitDefender's new phishing detector.

Self-learning Bayesian Filter. The advanced, self-learning Bayesian filter lets you classify messages as "Spam" or "Ham", with a single click in the BitDefender antispam toolbar. The filter will learn after just a few iterations, and you'll find yourself having to make fewer and fewer decisions as time goes by. Each tag you assign will improve the filter's accuracy. Your filter sensitivity settings can be as high or as low as you like.

Heuristic, URL, White List/Black List, Charset and Image Filters. Five types of filters further refine your control over e-mail. The heuristic filter checks mail for characteristics of spam. The White List/Black List filter will reject mail from known spammer addresses and let your friends' mail through. The URL filter blocks mail containing malicious links while the charset filter blocks mail written with “strange” characters. The Image filter can decide whether images embedded in e-mails are specific to spam.

Hassle-Free. You'll only be notified of the arrival of legitimate messages. Spam will collect silently in your "Junk" folder, to be examined or discarded at your leisure.

Compatibility and Outlook(tm) integration. BitDefender antispam is compatible with all e-mail clients. The BitDefender antispam toolbar in Microsoft Outlook and Outlook Express allows users to filter mail and contacts without exiting Outlook.

3.3. Firewall

The Firewall module protects your data and your privacy by filtering the incoming and outgoing traffic, controlling cookies, blocking malicious scripts and “XXX-dialer” type programs.

Internet Traffic Control. Define exactly which incoming or outgoing connections to permit/deny. Define rules regarding specific protocols, ports, applications and/or remote addresses.

Enhanced Internet Application Control. Alerts the users about any application trying to access the Internet. You will be notified whether the applications demanding network access are trustworthy, so you can make informed decisions.

Comprehensive Privacy Control. The firewall filters incoming and outgoing cookie type files, keeping your identity and preferences confidential when you're browsing the Internet.

Active Content Control. Proactively blocks any potentially malicious application such as: ActiveX, Java Applets or Java Scripts type codes.

Dial Control. A configurable anti-dialer prevents malicious applications from running up a huge telephone bill at your expense.

3.4. Other Features

Hourly Updates. Your copy of BitDefender will be updated 24 times a day over the Internet, directly or through a Proxy Server. The product is able to repair itself if necessary, by downloading the damaged or missing files from BitDefender servers. BitDefender license owners benefit from free virus definition updates and free product upgrades.

24/7 Support. Offered online by qualified support representatives and an online database with answers to Frequently Asked Questions.

Rescue Disk. **BitDefender 9 Professional Plus** is delivered on a bootable CD (based on LinuxDefender), which can be used to disinfect a system without booting it.

4. BitDefender modules

BitDefender 9 Professional Plus contains the modules: **General**, **Antivirus**, **Antispam**, **Firewall** and **Update**.

4.1. General module

BitDefender comes fully configured for maximum security.

Essential status information about all the BitDefender modules is displayed in the General module. Here you can register your product and you can set the overall behavior of BitDefender.

4.2. Antivirus module

BitDefender protects you from viruses entering your system by scanning your files, e-mail messages, downloads and all other content as it enters your system. From the antivirus module you have access to all BitDefender antivirus settings and features.

Virus protection is divided into two categories:

- On-access scanning - prevents new viruses or spyware from entering your system. This is also called a virus shield - files are scanned as the user accesses them. BitDefender will, for example, scan a word document for viruses when you open it, and an e-mail message when you receive one. BitDefender scans "as you use your files" - on-access.

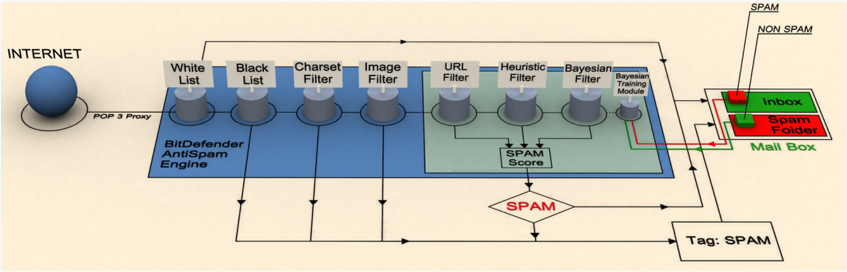
- On-demand scanning - detects already resident viruses or spyware in your system. This is the classic virus-scan initiated by the user - you choose what drive, folder or file BitDefender should scan, and BitDefender scans it - on-demand.

4.3. Antispam module

Spam is a growing problem, both for individuals and for organizations. It's not pretty, you wouldn't want your kids to see it, it can get you fired (for wasting too much time or from receiving porn in your office mail) and you can't stop people from sending it. The next best thing to that is, obviously, to stop receiving it. Unfortunately, Spam comes in a wide range of shapes and sizes, and there's a lot of it.

4.3.1. Working schema

The schema below shows the way BitDefender works.



Antispam Filters

The antispam filters from the above schema (White list, Black list, Charset filter, Image filter, URL filter, Heuristic filter and Bayesian filter) are used in conjunction by the BitDefender, to determine whether a certain piece of mail should make it to your **Inbox** or not.

Every e-mail that comes from the Internet is first checked with the White list/Black list filter. If the sender's address is found in the White list the e-mail is moved directly to your **Inbox**.

Otherwise the Black list filter will take over the e-mail to verify if the sender's address is on its list. The e-mail will be tagged as SPAM and moved in the **Spam** folder (located in Microsoft Outlook) if a match has been made.

Else, the Charset filter will check if the e-mail is written in Cyrillic or Asian characters. If so the e-mail will be tagged as SPAM and moved in the **Spam** folder.

If the e-mail is not written in Asian or Cyrillic it will be passed to the Image filter. The **Image filter** will detect all the e-mail messages containing attached images with spam content.

The URL filter will look for links and it will compare the links found with the links from the BitDefender database. In case of a match it will add a SPAM score to the e-mail.

The Heuristic filter will take over the e-mail and will perform a set of tests on all the message components, looking for words, phrases, links or other characteristics of SPAM. The result is that it will add a Spam score to the e-mail, too.

Note

If the e-mail is tagged as SEXUALLY EXPLICIT in the subject line, BitDefender will consider it SPAM.

The Bayesian filter module will further analyze the message, according to statistical information regarding the rate at which specific words appear in messages classified SPAM as compared to those declared NON-SPAM (by you or by the heuristic filter). A Spam score will be added to the e-mail.

If the aggregate score (URL score + heuristic score + Bayesian score) exceeds the SPAM score for a message (set by the user in the Antispam section as a tolerance level), the message is considered SPAM.

Important

If you are using other email client than Microsoft Outlook or Microsoft Outlook Express you should create a rule to move the e-mail messages tagged as SPAM by BitDefender to a custom quarantine folder. BitDefender appends the prefix `[SPAM]` to the subject of the messages considered to be SPAM.

4.3.2. Antispam filters

BitDefender Antispam Engine incorporates seven different filters that ensure your Inbox to be SPAM-free: White list, Black list, Charset filter, Image filter, URL filter, Heuristic filter and Bayesian filter.

Note

You can enable/disable each one of this filters in the Settings section from the **Antispam** module.

White list / Black list

Most people communicate regularly to a group of people or even receive messages from companies or organizations in the same domain. By using **friends or spammers list**, you can easily classify which people you want to receive e-mail from (friends) no matter what the message contains, or which people you never want to hear from again (spammers).

Note

White list / Black list are also known as **Friends list / Spammers list** correspondently.

The **Friends/Spammers list** can be managed from the Management Console or from the Antispam toolbar.

Note

We recommend that you add your friends' names and e-mail addresses to the **Friends list**. BitDefender does not block messages from those on the list; therefore, adding friends helps ensure that legitimate messages get through.

Charset filter

Most of the Spam messages are written in Cyrillic and / or Asian charsets. Configure this filter if you want to reject all the e-mail messages written in these charsets.

Image filter

Since avoiding heuristic filter detection has become quite a challenge, nowadays' inbox folders are full with more and more messages only containing an image with unsolicited content. To cope with this growing problem, BitDefender introduced the **Image filter** that compares the image signature from the e-mail with those from the BitDefender database. In case of a match the e-mail will be tagged as SPAM.

URL filter

Most of the Spam messages contain links to various web locations (which contain more advertising and the possibility to buy things, usually). BitDefender has a database, which contains links to these kinds of sites.

Every URL link in an e-mail message will be checked against the URL database. In case of a match a spam score will be added to the e-mail.

Heuristic filter

The **Heuristic filter** performs set of tests on all the message components, (i.e. not only the header but also the message body in either HTML or text format), looking for words, phrases, links or other characteristics of SPAM.

It detects also the e-mail messages with SEXUALLY EXPLICIT in the subject line. These messages are considered SPAM.

Note

Starting May 19th 2004, Spam that contains sexually oriented material must include the warning SEXUALLY EXPLICIT: in the subject line or face fines for violations of federal law.

Bayesian filter

The **Bayesian filter** module classifies messages according to statistical information regarding the rate at which specific words appear in messages classified SPAM as compared to those declared NON-SPAM (by you or by the heuristic filter).

This means, for example, if a certain four-letter word is seen to appear more often in SPAM, it is natural to assume there is an increased probability that the next incoming message that includes it actually IS SPAM. All relevant words within a message are taken into account. By synthesizing the statistical information, the overall probability for the whole message to be SPAM is computed.

This module presents another interesting characteristic: it is trainable. It adapts quickly to the type of messages received by a certain user, and stores information about all. To function effectively, the filter must be trained, meaning, to be presented with samples of SPAM and legitimate messages, much like a hound is primed to trace a certain scent. Sometimes the filter must be corrected too - prompted to adjust when it makes a wrong decision.

Important

You can correct the Bayesian module by using the **Is Spam** and **Not Spam** buttons from the "*Antispam toolbar*" (p. 98).

Note

Every time you perform an update:

- new image signatures will be added to the **Image filter**;
- new links will be added to the **URL filter**;
- new rules will be added to the **Heuristic filter**;

This will help increase the effectiveness of your Antispam engine.

Important

To protect you against spammers, BitDefender can perform automatic updates. Keep the **Automatic Update** option enabled.

4.4. Firewall module

The Firewall protects your computer from inbound and outbound unauthorized connection attempts. It is quite similar to a guard at your gate - it will keep a watchful eye on your Internet connection and keep track of who to allow access to the Internet and who to block.

A firewall is essential if you have a broadband or DSL connection. It is effective in blocking Trojan horses and other tools installed by hackers, who try to compromise your privacy and send your personal information, like credit card numbers, from your computer to the hacker.

4.5. Update module

New viruses&spyware are found and identified every day. This is why it is very important to keep BitDefender up to date with the latest virus&spyware signatures. By default, BitDefender automatically checks for updates every hour.

Updates come in the following ways:

- **Updates for the antivirus engines** - as new threats appear, the files containing virus signatures must be updated to ensure permanent up-to-date protection against them. This update type is also known as **Virus Definitions Update**.

- **Updates for the antispam engines** - new rules will be added to the heuristic and URL filters and new images will be added to the Image filter. This will help increase the effectiveness of your Antispam engine. This update type is also known as **Antispam Update**.

- **Updates for the antispyware engines** - new spyware signatures will be added to the database. This update type is also known as **Antispyware Update**.

- **Product upgrades** - when a new product version is released, new features and scan techniques are introduced to the effect of improving the product's performance. This update type is also known as **Product Update**.

Moreover, from the user's intervention viewpoint, we may take into account:

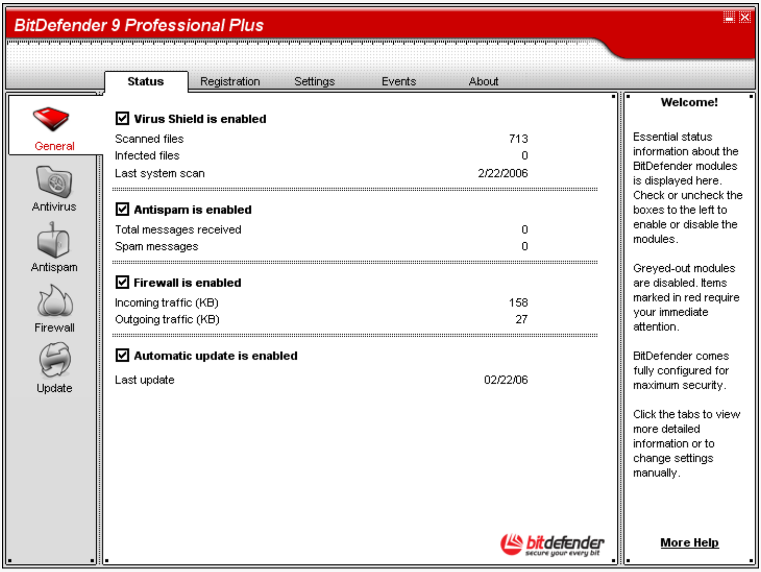
- Automatic update - the antivirus automatically contacts the BitDefender server in order to check if an update was released. If so, BitDefender is updated automatically. The automatic update can also be done anytime you want by clicking **Update now** from the Update module.
- Manual update - you must download and install the latest virus&spyware definitions manually.

Management console

5. Overview

BitDefender 9 Professional Plus was designed with a centralized management console, which allows the configuration of the protection options for all BitDefender modules. In other words, it is enough to open the management console in order to have access to all modules: **Antivirus**, **Antispam**, **Firewall** and **Update**.

To access the management console, use the Windows Start menu, by following the path **Start** -> **Programs** -> **BitDefender 9** -> **BitDefender 9 Professional Plus** or quicker, double click the **BitDefender icon** from the system tray.



☑ **Virus Shield is enabled**

Scanned files 713
Infected files 0
Last system scan 2/22/2006

☑ **Antispam is enabled**

Total messages received 0
Spam messages 0

☑ **Firewall is enabled**

Incoming traffic (KB) 158
Outgoing traffic (KB) 27

☑ **Automatic update is enabled**

Last update 02/22/06

Welcome!

Essential status information about the BitDefender modules is displayed here. Check or uncheck the boxes to the left to enable or disable the modules.

Greyed-out modules are disabled. Items marked in red require your immediate attention.

BitDefender comes fully configured for maximum security.

Click the tabs to view more detailed information or to change settings manually.

Management console

On the left side of the management console you can see the module selector:

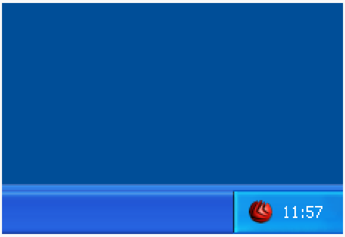
- General - in this section you can see a summary of all the BitDefender main settings, product details and contact information. Here you can also register the product.
- Antivirus - in this section you can configure the **Antivirus** module.

- Antispam - in this section you can configure the **Antispam** module.
- Firewall - in this section you can configure the **Firewall** module.
- Update - in this section you can configure the **Update** module.

On the right side of the management console you can see information regarding the section you are into. The **More Help** option, placed at the right bottom, opens the **Help** file.

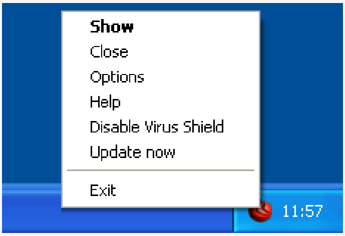
5.1. System tray

When the console is minimized, an icon will appear in the system tray:



System tray

If you double-click this icon, the management console will open.



Contextual menu

Also, by right-clicking it, a contextual menu containing the following options, will appear.

- **Show** - opens the management console.
- **Close** - minimizes the management console to system tray.
- **Options** - opens the Settings section of the management console.
- **Help** - opens the help file.
- **Enable / Disable Virus Shield** - enables / disables the on-access protection.
- **Update now** - performs an immediate update.

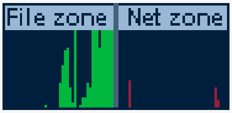
- **Exit** - shuts down the application. By selecting this option, the icon from the system tray will disappear and in order to access the management console, you will have to launch it again from the Windows Start menu.

Note

- The icon will turn into black, if you disable one or more of the BitDefender modules. This way you will know if some modules are disabled without opening the management console.
- The icon will blink when an update is available.

5.2. Scan activity bar

The **Scan activity bar** is a graphic visualization of the scanning activity on your system.



Activity bar

The green bars (the **File Zone**) show the number of scanned files per second, on a scale from 0 to 50.

The red bars displayed in the **Net Zone** show the number of Kbytes transferred (sent and received from the Internet) every second, on a scale from 0 to 100.

Note

The **Scan activity bar** will notify you when the Virus Shield or the Firewall is disabled with a red cross over the corresponding area (**File Zone** or **Net Zone**). This way you will know if you are protected without opening the management console.

When you no longer want to see the graphic visualization, just right-click it and select **Hide**.

Note

To completely hide this window, clear **Enable activity bar** option (from the **General** module, Settings section).

6. General module

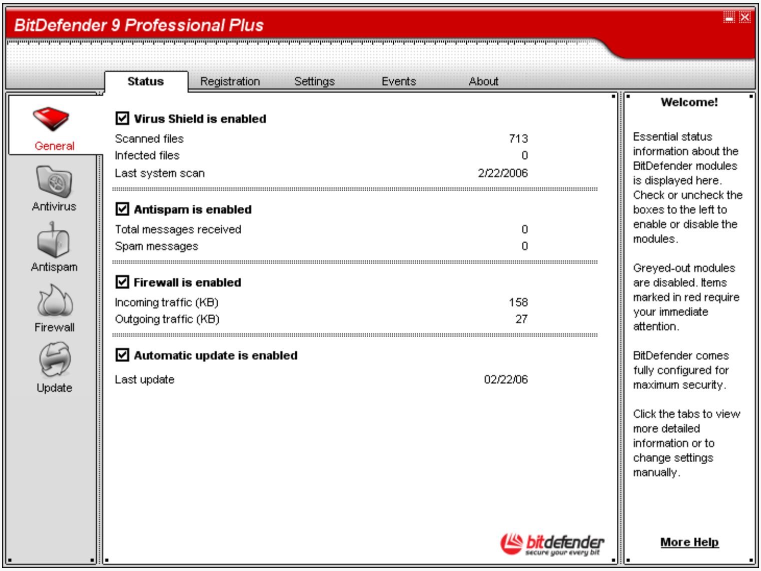
The **General** section of this user guide contains the following topics:

- General information
- Product registration
- Management console settings
- Events
- About

Note
For more details regarding the **General** module check the description of the “*General module*” (p. 35).

6.1. General information

To access this section click **Status** tab from the **General** module.



☑ **Virus Shield is enabled**

Scanned files	713
Infected files	0
Last system scan	2/22/2006

☑ **Antispam is enabled**

Total messages received	0
Spam messages	0

☑ **Firewall is enabled**

Incoming traffic (KB)	158
Outgoing traffic (KB)	27

☑ **Automatic update is enabled**

Last update	02/22/06

Welcome!

Essential status information about the BitDefender modules is displayed here. Check or uncheck the boxes to the left to enable or disable the modules.

Greyed-out modules are disabled. Items marked in red require your immediate attention.

BitDefender comes fully configured for maximum security.

Click the tabs to view more detailed information or to change settings manually.

General information

In this section you can review information regarding the product status.

To enable/disable the main BitDefender features select/clear the check boxes corresponding to them.

Warning
Items marked in red require your immediate attention.

6.1.1. Virus Shield

It provides real-time continuous protection from viruses and other malicious threats. The number of scanned files, infected files and the date of the last system scan are displayed.

Note
To prevent viruses from infecting your computer keep **Virus Shield** enabled.

Warning

We strongly recommend you a full system scan at least once a week. In order to perform a full system scan, access the **Antivirus** module, Virus Scan section, check **Local Drives** and click **Scan**.

6.1.2. Antispam

Spam is a growing problem, both for individuals and for organizations. It comes in a wide range of shapes and sizes, and there's a lot of it. The **Antispam** module works with all e-mail clients and can be configured from the Management Console (**Antispam** section).

Moreover it integrates directly with Microsoft Outlook and Microsoft Outlook Express allowing a smooth interaction with the Antispam filters through an intuitive and easy-to-use interface.

Note

To prevent Spam from entering your Inbox, keep **Antispam filter** enabled. See how BitDefender Antispam is working.

6.1.3. Firewall

The Firewall protects you against Internet attacks. The firewall rules prevent hackers and malicious software from compromising your computer or your personal data. The figures shown represent the Internet traffic during this session.

Note

To be protected against Internet attacks keep the **Firewall** enabled.

6.1.4. Automatic Update

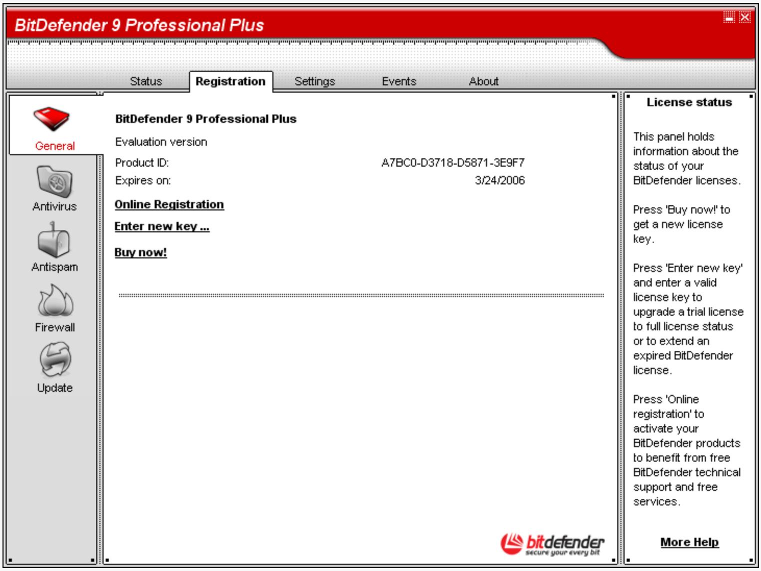
New viruses are found and identified every day. This is why it is very important to keep BitDefender up to date with the latest virus signatures. It displays the date of the last update.

Note

To protect your critical data, BitDefender can perform automatic updates. Keep the **Automatic update** option enabled.

6.2. Product registration

To access this section click **Register** tab from the **General** module.



BitDefender 9 Professional Plus

Evaluation version

Product ID: A7BC0-D3718-D5871-3E9F7

Expires on: 3/24/2006

Online Registration

Enter new key ...

Buy now!

License status

This panel holds information about the status of your BitDefender licenses.

Press 'Buy now!' to get a new license key.

Press 'Enter new key' and enter a valid license key to upgrade a trial license to full license status or to extend an expired BitDefender license.

Press 'Online registration' to activate your BitDefender products to benefit from free BitDefender technical support and free services.

More Help

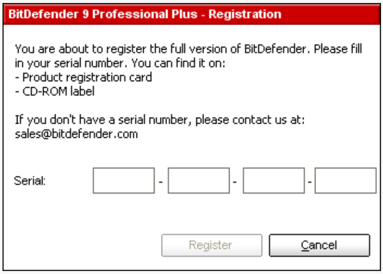
Product registration

This section contains information about the status of your BitDefender license. Here you can register the product and you can see the expiring date.

The product is delivered with a trial registration key valid for thirty days. At the end of the trial period, if you want to purchase the product you have to provide a new license key. Click **Buy now** to get a new **License Key** from the BitDefender online store.

Click **Online registration** to activate your BitDefender product in order to benefit from free BitDefender technical support and other services.

To modify the default license key click **Enter new key**. The following window will open:



BitDefender 9 Professional Plus - Registration

You are about to register the full version of BitDefender. Please fill in your serial number. You can find it on:
- Product registration card
- CD-ROM label

If you don't have a serial number, please contact us at: sales@bitdefender.com

Serial: □ - □ - □ - □

Enter registration key

Type in the license key in the **Serial** field. Click **Register** to finish the registration process.

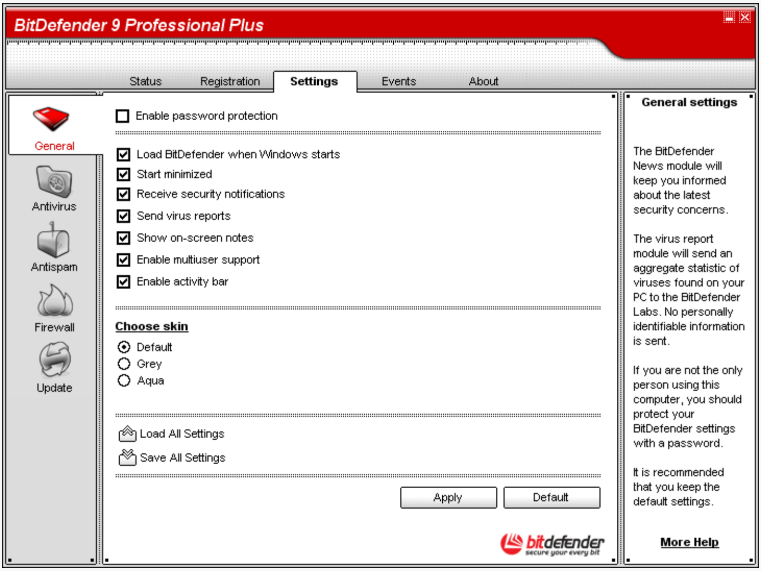
If you mistype the license key you will be prompted to re-enter it.

If you type in a valid license key a success message box appears.

In the **Registration** section now, you can see the expiring date of the new license key.

6.3. Management console settings

To access this section click **Settings** tab from the **General** module.



☐ Enable password protection

☑ Load BitDefender when Windows starts
☑ Start minimized
☑ Receive security notifications
☑ Send virus reports
☑ Show on-screen notes
☑ Enable multiuser support
☑ Enable activity bar

Choose skin
● Default
○ Grey
○ Aqua

Load All Settings
Save All Settings

General settings

The BitDefender News module will keep you informed about the latest security concerns.

The virus report module will send an aggregate statistic of viruses found on your PC to the BitDefender Labs. No personally identifiable information is sent.

If you are not the only person using this computer, you should protect your BitDefender settings with a password.

It is recommended that you keep the default settings.

Management console settings

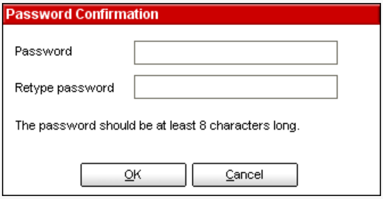
Here you can set the overall behavior of BitDefender. By default, BitDefender is loaded at Windows startup and then runs minimized in the taskbar.

The following options are available:

- **Enable password protection** - enables setting a password in order to protect the BitDefender Management Console configuration;

  Note
  If you are not the only person using this computer, it is recommended that you protect your BitDefender settings with a password.

  If you select this option, the next window will appear:



Password Confirmation

Password

Retype password

The password should be at least 8 characters long.

Enter password

Type in the password in the **Password** field, re-type it in the **Retype password** field and click **OK**.

From now on, if you want to change the BitDefender configuration options, you will be asked to introduce the password.

Important

If you forgot the password you will have to repair the product in order to modify the BitDefender configuration.

- **Load BitDefender when Windows starts** - automatically launches BitDefender at system startup.

Note

We recommend you to keep this option selected.

- **Start minimized** - minimizes the BitDefender management console after it has been loaded at system startup. Only the BitDefender Icon will appear in the system tray.
- **Receive security notifications** - receives from time to time security notifications regarding virus outbreaks, sent by the BitDefender server.
- **Send virus reports** - sends to the BitDefender Labs reports regarding viruses identified in your computer. It helps us keep track of virus-outbreaks.

  The reports will contain no confidential data, such as your name, IP address or others, and will not be used for commercial purposes. The information supplied will contain only the virus name and will be used solely to create statistic reports.
- **Show on-screen notes** - shows pop-up windows regarding the product status.
- **Enable multiuser support** - allows other users that may be using this computer to have their own settings for BitDefender.

Note

This option can only be enabled or disabled by users with administrator rights on the local machine.

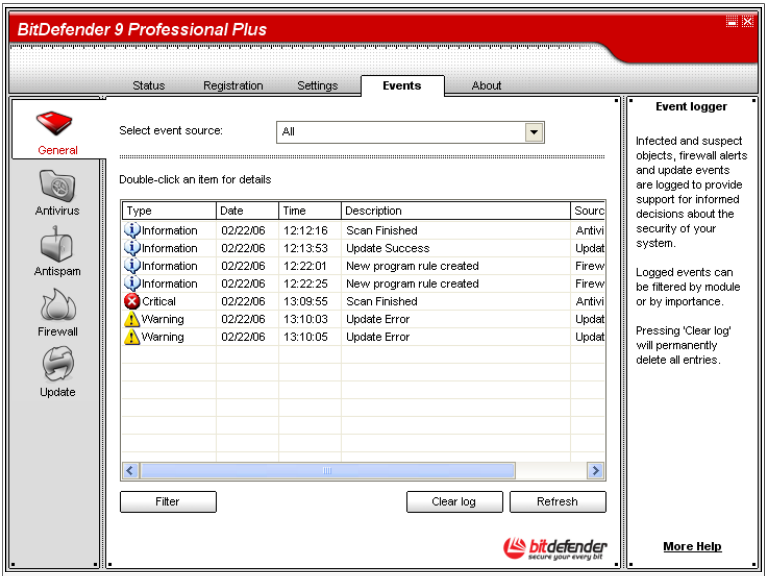
- **Enable activity bar** - enables/disables the “ *Scan activity bar* ” (p. 45).
- **Choose skin** - allows you to select the color of the management console. The skin represents the background image on the interface. In order to select a different skin, click the corresponding color.

Use the **Save All Settings** / **Load All Settings** buttons to save / load the settings you have made for BitDefender to a desired location. This way you can use the same settings after you reinstall or repair your BitDefender product.

Click **Apply** to save the changes. If you click **Default** you will load the default settings.

6.4. Events

To access this section click **Events** tab from the **General** module.



Select event source: All

Double-click an item for details

Type	Date	Time	Description	Sourc
ℹ Information	02/22/06	12:12:16	Scan Finished	Antivi
ℹ Information	02/22/06	12:13:53	Update Success	Updat
ℹ Information	02/22/06	12:22:01	New program rule created	Firew
ℹ Information	02/22/06	12:22:25	New program rule created	Firew
✖ Critical	02/22/06	13:09:55	Scan Finished	Antivi
⚠ Warning	02/22/06	13:10:03	Update Error	Updat
⚠ Warning	02/22/06	13:10:05	Update Error	Updat

Event logger

Infected and suspect objects, firewall alerts and update events are logged to provide support for informed decisions about the security of your system.

Logged events can be filtered by module or by importance.

Pressing 'Clear log' will permanently delete all entries.

Events

In this section all the events generated by BitDefender are displayed.

There are 3 types of events: ℹ **Information**, ⚠ **Warning** and ✖ **Critical**.

Examples of events:

- **Information** - when an e-mail was scanned;
- **Warning** - when a suspected file was detected;
- **Critical** - when an infected file was detected.

For each event the following information are offered: the date and the time when the event occurred, a small description and its source (**Antivirus**, **Firewall** or **Update**). Double-click an event to see its properties.

You can filter these events in 2 ways (by type or by source):

- Click **Filter** to select what types of event to display.
- Select the event source from the drop-down menu.

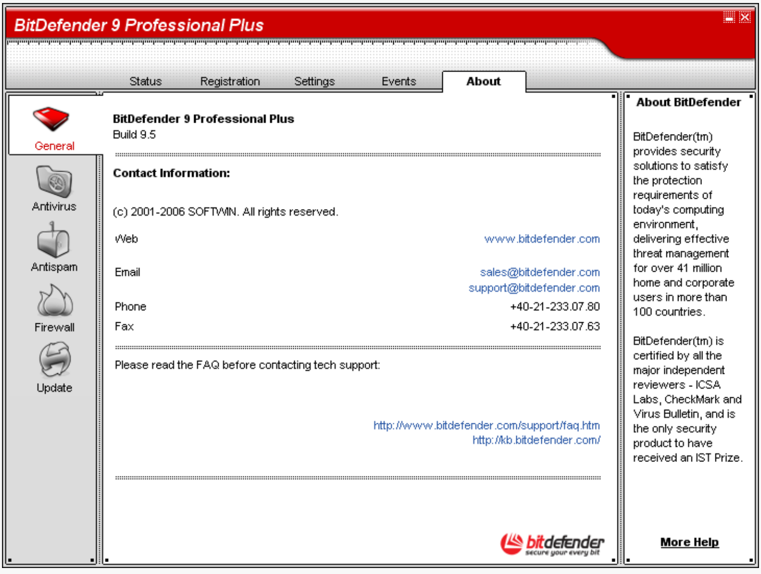
If the management console is open at the **Events** section and at the same time an event occurs you must click **Refresh** to see that event.

To delete all the events from the list click **Clear log**.

6.5. About

To access this section click **About** tab in the **General** module.

In this section you can find the contact information and the product details.



BitDefender 9 Professional Plus
Build 9.5

Contact Information:

(c) 2001-2006 SOFTWIN. All rights reserved.

Web	www.bitdefender.com
Email	sales@bitdefender.com support@bitdefender.com
Phone	+40-21-233.07.80
Fax	+40-21-233.07.63

Please read the FAQ before contacting tech support:

http://www.bitdefender.com/support/faq.htm
http://kb.bitdefender.com/

About BitDefender

BitDefender(tm) provides security solutions to satisfy the protection requirements of today's computing environment, delivering effective threat management for over 41 million home and corporate users in more than 100 countries.

BitDefender(tm) is certified by all the major independent reviewers - ICSA Labs, CheckMark and Virus Bulletin, and is the only security product to have received an IST Prize.

General information

BitDefender provides security solutions to satisfy the protection requirements of today's computing environment, delivering effective threat management for over 41million home and corporate users in more than 100 countries.

BitDefender is certified by all the major independent reviewers - **ICSA Labs**, **CheckMark** and **Virus Bulletin**, and is the only security product to have received an **IST Prize**.

7. Antivirus module

The **Antivirus** section of this user guide contains the following topics:

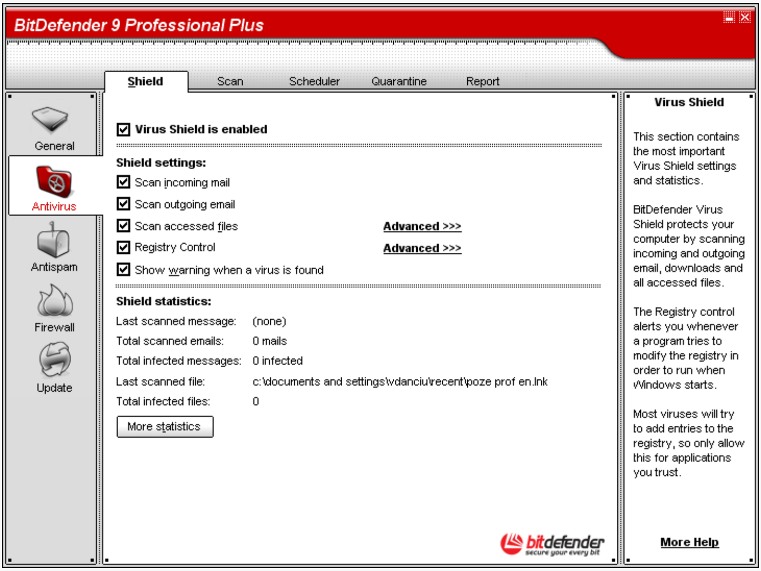
- On-access scanning
- On-demand scanning
- Scheduled scanning
- Quarantine
- Report

Note

For more details regarding the **Antivirus** module check the description of the "*Antivirus module*" (p. 35).

7.1. On-access scanning

To access this section click **Shield** tab from the **Antivirus** module.



☑ **Virus Shield is enabled**

Shield settings:

☑ Scan incoming mail

☑ Scan outgoing email

☑ Scan accessed files **Advanced >>>**

☑ Registry Control **Advanced >>>**

☑ Show warning when a virus is found

Shield statistics:

Last scanned message:	(none)
Total scanned emails:	0 mails
Total infected messages:	0 infected
Last scanned file:	c:\documents and settings\vdanciu\recent\poze prof en.lnk
Total infected files:	0

More statistics

Virus Shield

This section contains the most important Virus Shield settings and statistics.

BitDefender Virus Shield protects your computer by scanning incoming and outgoing email, downloads and all accessed files.

The Registry control alerts you whenever a program tries to modify the registry in order to run when Windows starts.

Most viruses will try to add entries to the registry, so only allow this for applications you trust.

More Help

Virus Shield

In this section you can configure the **Virus Shield** and you can view information regarding its activity. The **Virus Shield** protects your computer by scanning e-mail messages, downloads and all accessed files.

Note

To prevent viruses from infecting your computer keep the **Virus Shield** enabled.

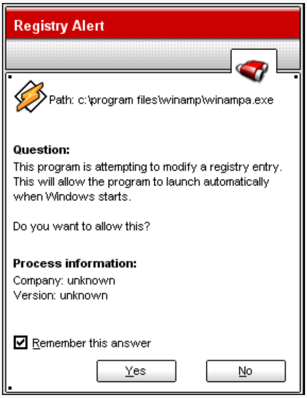
In the bottom side of the section you can see the **Virus Shield** statistics about files and e-mail messages scanned. Click **More statistics** if you want to see a more explained window regarding these statistics.

7.1.1. Registry Control

A very important part of the Windows operating system is called the **Registry**. This is where Windows keeps its settings, installed programs, user information and so on.

The **Registry** is also used to define which programs should be launched automatically when Windows is started. Viruses often use this in order to be automatically launched when the user restarts his computer.

Registry Control keeps an eye on the Windows Registry - this is again useful for detecting Trojan horses. It will alert you whenever a program will try to modify a registry entry in order to be executed at Windows start-up.



Registry Alert

Path: c:\program files\winamp\winampa.exe

Question:
This program is attempting to modify a registry entry. This will allow the program to launch automatically when Windows starts.

Do you want to allow this?

Process information:
Company: unknown
Version: unknown

☑ Remember this answer

Registry Alert

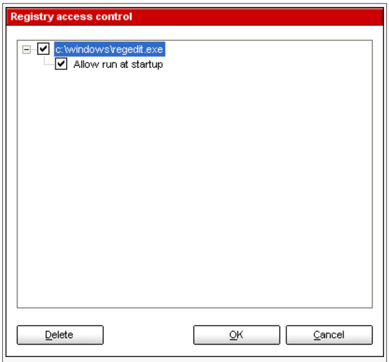
You can deny this modification by clicking **No** or you can allow it by clicking **Yes**.

If you want BitDefender to remember your answer you must select the checkbox: **Remember this answer**.

Note

Your answers will be the basis of the rule-list.

If you want to see the registry entries list, click **Advanced >>>** corresponding to **Registry Control**.



Registry access control

For each application a small expandable menu will be created; it contains all the modifications to the registry.

To delete a registry entry, just select it and click **Delete**. To temporarily deactivate a registry entry without deleting it, clear the checkbox corresponding to it.

Note

BitDefender will usually alert you when you install new programs that need to run after the next startup of your computer. In most cases, these programs are legitimate and can be trusted

7.1.2. Most important settings

To select an option, select the corresponding checkbox.

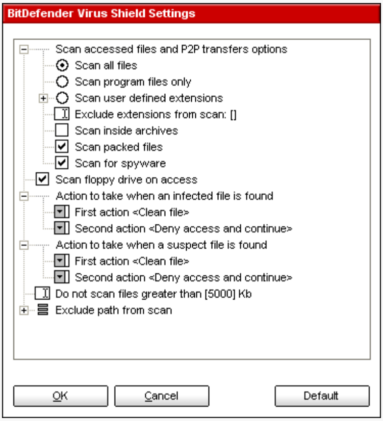
- **Scan incoming email** - scans all the incoming e-mail messages.
- **Scan outgoing email** - scans all the outgoing e-mail messages.
- **Scan accessed files** - scans all the accessed files.
- **Show warning when a virus is found** - opens an alert window when a virus is found in a file or in an e-mail message.

  For an infected file the alert window will contain the name of the virus, the path to it, the action taken by BitDefender and a link to the BitDefender site where you can find more information about it. For an infected e-mail the alert window will contain also information about the sender and the receiver.

  In case a suspicious file is detected you can launch a wizard from the alert window that will help you to send that file to the BitDefender Lab for further analysis. You can type in your e-mail address to receive information regarding this report.

7.1.3. Other settings

Advanced users might want to take advantage of the scan-settings BitDefender offers. The scanner can be set to skip file extensions, directories or archives that you know to be harmless. Click **Advanced >>>** corresponding to **Scan accessed files** to explore these settings.



BitDefender Virus Shield Settings

- ⊟ Scan accessed files and P2P transfers options
  - ● Scan all files
  - ○ Scan program files only
  - ⊞ ○ Scan user defined extensions
  - Exclude extensions from scan: []
  - □ Scan inside archives
  - ☑ Scan packed files
  - ☑ Scan for spyware
- ☑ Scan floppy drive on access
- ⊟ Action to take when an infected file is found
  - First action <Clean file>
  - Second action <Deny access and continue>
- ⊟ Action to take when a suspect file is found
  - First action <Clean file>
  - Second action <Deny access and continue>
- Do not scan files greater than [5000] Kb
- ⊞ Exclude path from scan

Virus Shield settings

Click the box with "+" to open an option or the box with "-" to close an option.

You can observe that some scan options, although the "+" sign appears, cannot be opened. The reason is that these options weren't selected yet. You will observe that if you select them, they can be opened.

- **Scan accessed files and P2P transfers options** - scans the accessed files and the communications through Instant Messaging Software applications (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Further on, select the type of the files you want to be scanned.

  The following options are available:

Option	Description
Scan all files	All the accessed files will be scanned, regardless their type.
Scan program files only	Only the program files will be scanned. This means only the files with the following extensions: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml` and `.nws`.

Option	Description
Scan user defined extensions	Only the files with the extensions specified by the user will be scanned. These extensions must be separated by ";".
Exclude extensions from scan	The files with the extensions specified by the user will NOT be scanned. These extensions must be separated by ";".
Scan inside archives	The accessed archives will be scanned. With this option on, the computer will slow down.
Scan packed files	All packed files will be scanned.
Scan for spyware	Scans for spyware applications. These files will be treated as infected files. Software that includes adware components might stop working if this option is enabled.

- **Scan floppy drive on access** - scans the floppy drive, when it is accessed.
- **Action to take when an infected file is found** - select from the drop-down menu the first action to take on infected files. BitDefender allows selecting two actions in case an infected file is found.

  You can select one of the following actions:

Action	Description
Deny access and continue	In case an infected file is detected, the access to this will be denied.
Clean file	Disinfects the infected file.
Delete file	Deletes the infected files immediately, without any warning.
Move file to quarantine	Move the infected files into the quarantine.

- **Second action to take when first fails** - select from the drop-down menu the second action to take on infected files, in case the first action fails.

  You can select one of the following actions:

Action	Description
Deny access and continue	In case an infected file is detected, the access to this will be denied.

Action	Description
Delete file	Deletes the infected files immediately, without any warning.
Move file to quarantine	Move the infected files into the quarantine.

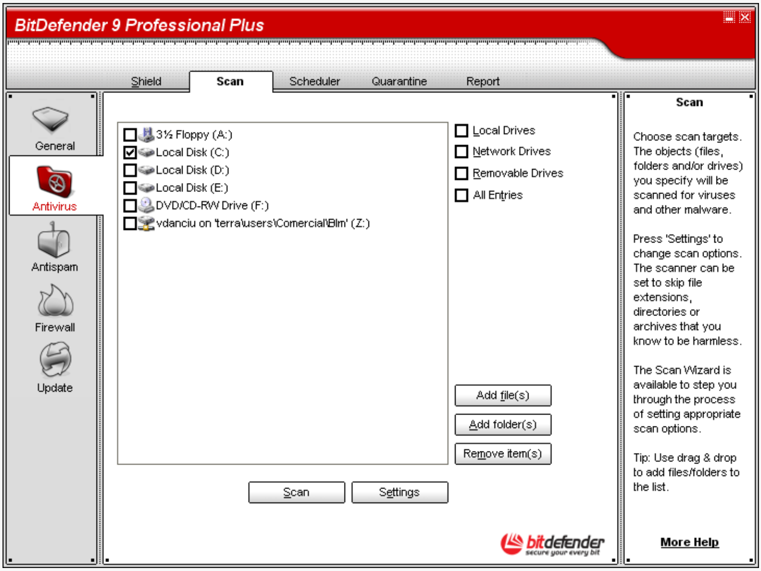
The same actions as for infected files are available for suspected ones.

- **Do not scan files greater than** - type in the maximum size of the files to be scanned. If the size is 0 Kb, all files will be scanned
- **Exclude path from scan** - click "+" corresponding to this option in order to specify a folder that will be excluded from scanning. The consequence of this will be that the option will expand and a new option, `New item`, will appear. Click the corresponding checkbox of the new item and from the exploring window select the folder you want to be excluded from scanning.

Click **OK** to save the changes or click **Default** to load the default settings.

7.2. On-demand scanning

To access this section click **Scan** tab from the **Antivirus** module.



□ 3½ Floppy (A:)
☑ Local Disk (C:)
□ Local Disk (D:)
□ Local Disk (E:)
□ DVD/CD-RW Drive (F:)
□ vdanciu on 'terra\users\Comercial\Blm' (Z:)

□ Local Drives
□ Network Drives
□ Removable Drives
□ All Entries

Scan

Choose scan targets. The objects (files, folders and/or drives) you specify will be scanned for viruses and other malware.

Press 'Settings' to change scan options. The scanner can be set to skip file extensions, directories or archives that you know to be harmless.

The Scan Wizard is available to step you through the process of setting appropriate scan options.

Tip: Use drag & drop to add files/folders to the list.

Virus Scan

In this section you can configure BitDefender to scan your computer.

The main objective for BitDefender is to keep your computer clean of viruses. This is first and foremost done by keeping new viruses out of your computer and by scanning your e-mail messages and any new files downloaded or copied to your system.

There is a risk that a virus is already lodged in your system, before you even install BitDefender. This is why it's a very good idea to scan your computer for resident viruses after you've installed BitDefender. And it's definitely a good idea to frequently scan your computer for viruses.

BitDefender allows four types of on demand scan:

- Immediate scanning - there are a few steps to follow in order to scan your computer for viruses;
- Contextual scanning - right-click on a file or a folder and select BitDefender Antivirus v9;
- Drag& Drop scanning - drag and drop a file or a folder over the Scan Activity Bar;
- Scheduled scanning - you can program BitDefender to scan your system for viruses periodically.

7.2.1. Immediate scanning

To scan your computer for viruses, please follow the next steps:

Step 1/5 - Close all open programs

In order for BitDefender to make a complete scanning, you need to shut down all open programs. Especially your email-client (i.e. Outlook, Outlook Express or Eudora) is important to shut down.

Step 2/5 - Make sure that BitDefender knows the latest viruses

Before you let BitDefender scan your computer you should make sure that BitDefender is up to date with its virus signatures, since new viruses are found and identified every day. You can verify when the last update was made in the upper side of the Update module.

Step 3/5 - Choose scan targets

In the management console, enter the **Antivirus** module and click Scan tab. By default, the section contains an image of the system's partition structure. Besides this, some buttons and scan options can also be observed.

The section contains the following buttons:

- **Add file(s)** - opens, a browsing window, where you can select the file(s), you want to scan.
- **Add folder(s)** - same as above, but you select which folder(s) you want BitDefender to scan instead of which file(s).

Note

You can also use drag and drop to add files/folders to the list.

- **Remove item(s)** - removes the file(s) / folder(s) that has been previously selected from the list of objects to be scanned.

Note

Only the file(s) / folder(s) that were added afterwards can be deleted, but not those that were automatically "seen" by BitDefender.

- **Settings** - opens a window where you can specify which files to be scanned, the action on the infected files, generating alert messages, saving scan results in report files.

- **Scan** - launches the system scanning, taking in account the selected scan options.

Besides the buttons explained above there are also some options that allow the fast selection of the scan locations.

- **Local drives** - to scan the local drives.
- **Network drives** - to scan all network drives.
- **Removable drives** - to scan the removable drives (CD-ROM, floppy-disk unit).
- **All entries** - to scan all drives, no matter if they are local, in the network or removable.

Note

If you want to scan your entire computer for viruses, select the checkbox corresponding to **All entries**.

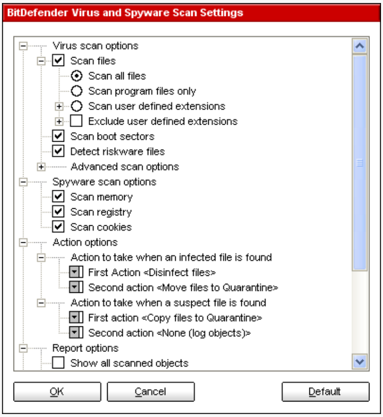
Important

If you are not that familiar with computers, now is the time to just click the **Scan** button. BitDefender will start the scanning of your computer using the standard settings, which are sufficient.

Step 4/5 - Select the scan options

Advanced users might want to take advantage of the scan-settings BitDefender offers. The scanner can be set to skip file extensions, directories or archives that you know to be harmless. This may greatly reduce scanning times and improve your computer responsiveness during a scan.

Click **Settings** from the Scan section to explore these options.



BitDefender Virus and Spyware Scan Settings

- Virus scan options
  - ☑ Scan files
    - ● Scan all files
    - ○ Scan program files only
    - ○ Scan user defined extensions
    - □ Exclude user defined extensions
  - ☑ Scan boot sectors
  - ☑ Detect riskware files
  - Advanced scan options
- Spyware scan options
  - ☑ Scan memory
  - ☑ Scan registry
  - ☑ Scan cookies
- Action options
  - Action to take when an infected file is found
    - First Action <Disinfect files>
    - Second action <Move files to Quarantine>
  - Action to take when a suspect file is found
    - First action <Copy files to Quarantine>
    - Second action <None (log objects)>
- Report options
  - □ Show all scanned objects

Scan settings

The scan options are organized like an expandable menu very much like the exploring ones from Windows.

The scan options are grouped in five categories:

- **Virus scan options**
- **Spyware scan options**
- **Action options**
- **Report options**
- **Other options**

Note

Click the box with "+" to open an option or the box with "-" to close an option.

- Specify the type of objects to be scanned (archives, e-mail messages and so on) and other options. This is made through the selection of certain options from **Virus scan options** category.

  The following detection options are available:

Option		Description
Scan files	**Scan all files**	Scans all files, regardless of their type.
	Scan program files only	Only the program files will be scanned. This means only the files with the following extensions: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`;

Option		Description
		`sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`; `prc`; `url`; `smm`; `pdf`; `msi`; `ini`; `csc`; `cmd`; `bas`; `eml` and `nws`.
	Scan user defined extensions	Scans only the files with the extensions specified by the user. These extensions must be separated by ";".
	Exclude user defined extensions	The files with the extensions specified by the user will NOT be scanned. These extensions must be separated by ";".
Scan boot sectors		Scans the system's boot sector.
Detect riskware files		Scans for threats other than viruses, such as dialers and adware. These files will be treated as infected files. Software that includes adware components might stop working if this option is enabled.
Advanced scan options	**Open packed programs**	Scans packed files.
	Open archives	Scans inside archives.
	Open e-mail archives	Scans inside mail archives.
	Use heuristic detection	To use heuristic scanning of the files. The aim of heuristic scanning is to identify new viruses, based on certain patterns and algorithms, before a virus definition is found. False alarm messages can appear. When such a file is detected it is classified as suspicious. In these cases, we recommend you to send the file to the BitDefender lab to be analyzed.
	Detect incomplete virus bodies	Detects incomplete virus bodies.

- Specify the spyware scan target (processes, cookies and/or memory). This is made through the selection of certain options from **Spyware scan options** category.

  The following detection options are available:

Option	Description
Scan processes	Scans processes.
Scan cookies	Scans cookie files.
Scan registry	Scans registry entries.

- Specify the action on infected or suspicious files. Open **Action options** category in order to see all possible actions on these files.

  Select the actions to take when an infected or a suspected file is detected. You can specify different actions for infected and suspected files. You can also select a second action if the first fails.

Action	Description
None (log objects)	No action will be taken on infected files. These files will appear in the report file.
Prompt user for action	When an infected file is detected, a window will appear prompting the user to select the action on that file. Depending on the importance of that file, you can select to disinfect it, isolate it in the quarantine zone or delete it.
Disinfect files	Disinfects the infected file.
Delete files	Deletes the infected files immediately, without any warning.
Rename files	Changes the extension of the infected files. The new extension of the infected files will be `.vir`. By renaming the infected files, the possibility of executing and thus of spreading the infection is removed. At the same time they can be saved for further examination and analysis.
Copy files to Quarantine	Copies the infected files into the quarantine. This means practically duplicating the infected file and the copy of this file will appear in the quarantine, but the infected file will not be moved from the initial location.
Move files to Quarantine	Moves the infected files into the quarantine.

- Specify the options for the report files. Open **Report options** category in order to see all possible options.

Option		Description
Show all scanned files		Lists all scanned files and their status (infected or not) in a report file. With this option on, the computer will slow down.
Create report file	**Report file name** `vscan.log`	This is an edit field that allows changing the name of the report file. Select this option and type in a new name.
	Limit report size to [x] KB	Limits the size of the report file. Type in the maximum file size.

Note
The report files can be seen in the Report section from the **Antivirus** module.

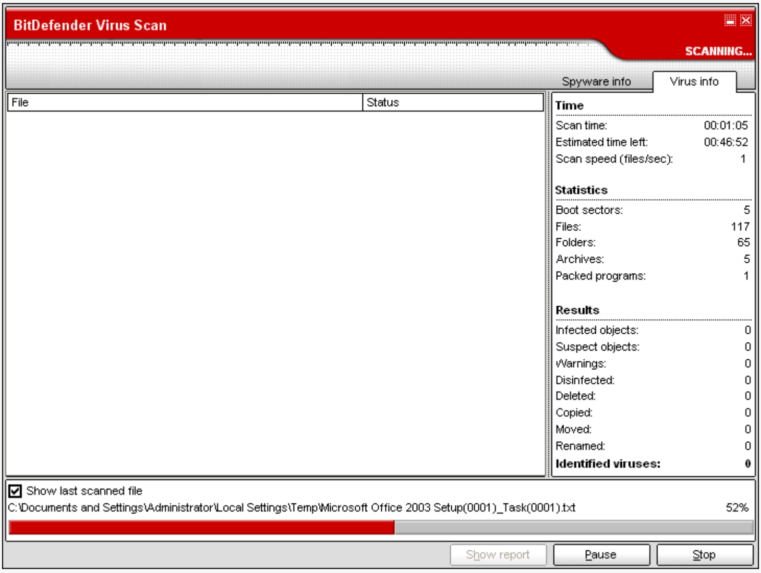
- Specify the other options. Open **Other options** category from where you can select the following options:

Option	Description
Run the task with Low priority	Decreases the priority of the scan process. You will allow other programs to run faster and increase the time needed for the scan process to finish.
Shut down the PC when scan is completed	Shut down the computer after the scan process has finished.
Submit suspect files to BitDefender Lab	You will be prompted to submit all suspect files to BitDefender lab after the scan process has finished.
Minimize scan window on start to systray	Minimizes the scan window to system tray. Double-click the BitDefender icon to open it.
Promp for reboot	If actions require reboot, prompt users for immediate reboot.

Click **OK** to save the changes or click **Default** to load the default settings.

Step 5/5 - Scan for viruses

With the scan options selected, all you have to do is to effectively start the system scanning. For that, just click **Scan**. The scan window will appear:



Time

Scan time:	00:01:05
Estimated time left:	00:46:52
Scan speed (files/sec):	1

Statistics

Boot sectors:	5
Files:	117
Folders:	65
Archives:	5
Packed programs:	1

Results

Infected objects:	0
Suspect objects:	0
Warnings:	0
Disinfected:	0
Deleted:	0
Copied:	0
Moved:	0
Renamed:	0
Identified viruses:	**0**

☑ Show last scanned file

C:\Documents and Settings\Administrator\Local Settings\Temp\Microsoft Office 2003 Setup(0001)_Task(0001).txt 52%

Virus Scan

While scanning, BitDefender will show you its progress and alert you if any threats are found. In the right, you can see statistics about the scanning process. Depending on the scan target, spyware and/or virus information is available. If both are available, click the corresponding tab to learn more about the spyware or virus scanning process.

Select the check box corresponding to **Show last scanned file** and only the information about the last scanned file will be visible.

Note

The scanning process may take a while, depending on the size of your hard disk drive.

Three buttons are available:

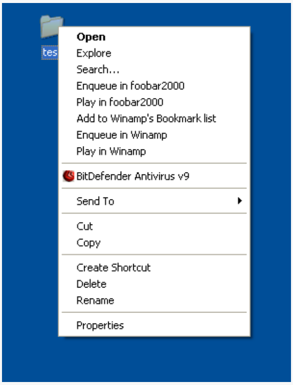
- **Stop** - opens a new window from where you can end the scan process. Click **Yes&Close** to exit the scan window.
- **Pause** - stops temporally the scan process - you can continue it by clicking **Resume**.
- **Show report** - opens the scan report.

Note
The report file is saved automatically in the Report section from the **Antivirus** module.

An icon will appear in the system tray when a scan process is running.

7.2.2. Contextual scanning

Right-click the file or folder you want scanned and select the **BitDefender Antivirus v9**.

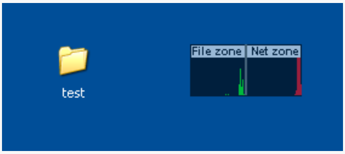


Contextual Scan

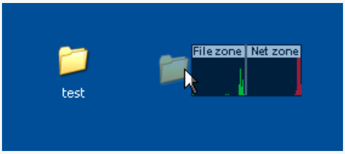
A report file named `vscan.log` will be created and you can open it from the Report section, **Antivirus** module.

7.2.3. Drag and Drop Scanning

Drag the file or folder you want scanned and drop it over the **Scan Activity Bar**, like in the pictures below.



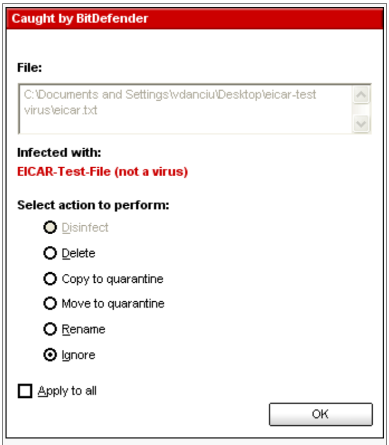
Drag the file



Drop the file

A report file named `activbar.log` will be created and you can open it from the Report section, **Antivirus** module.

In both alternative scanning (contextual and drag&drop scanning) the scan window will appear. If a virus is detected, an alert window will prompt you to select the action on the infected file.



Caught by BitDefender

File:

C:\Documents and Settings\vdanciu\Desktop\eicar-test virus\eicar.txt

Infected with:

EICAR-Test-File (not a virus)

Select action to perform:

○ Disinfect

○ Delete

○ Copy to quarantine

○ Move to quarantine

○ Rename

● Ignore

□ Apply to all

Action Selection

You can view the name of the file and the name of the virus.

Select one of the following actions to take on the infected file:

- **Disinfect** - disinfects the infected file;
- **Delete** - deletes the infected file;
- **Copy to quarantine** - copies the infected file into the quarantine;
- **Move to quarantine** - moves the infected file into the quarantine;
- **Rename** - changes the extension of the infected files. The new extension of the infected files will be `.vir`.
- **Ignore** - ignores the infection. No action will be taken on the infected file.

If you scan a folder, and you wish the action on the infected files to be the same for all, select the checkbox corresponding to **Apply to all**.

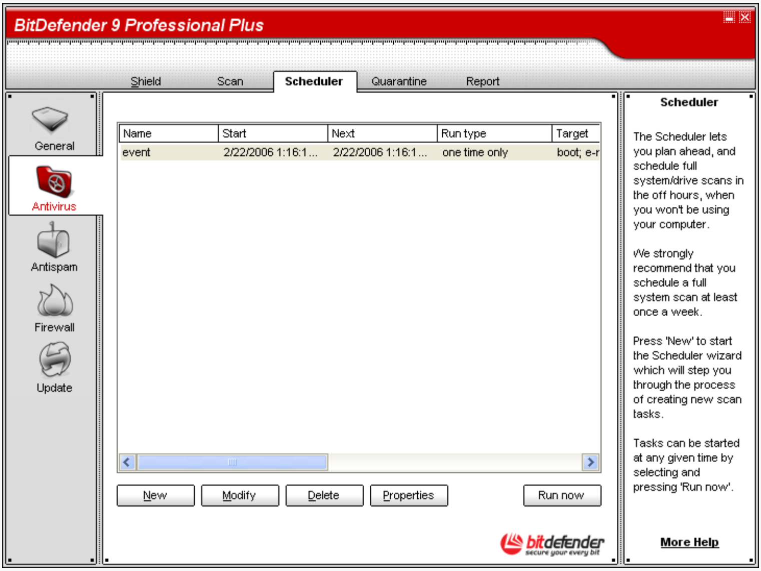
Note

If the **Disinfect** option is not enabled, it means the file cannot be disinfected. The best choice is to isolate it in the quarantine zone and send it to us for analysis or delete it.

Click **OK**.

7.2.4. Scheduled scanning

To access this section click **Scheduler** tab from the **Antivirus** module.



Name	Start	Next	Run type	Target
event	2/22/2006 1:16:1...	2/22/2006 1:16:1...	one time only	boot; e-r

Scheduler

The Scheduler lets you plan ahead, and schedule full system/drive scans in the off hours, when you won't be using your computer.

We strongly recommend that you schedule a full system scan at least once a week.

Press 'New' to start the Scheduler wizard which will step you through the process of creating new scan tasks.

Tasks can be started at any given time by selecting and pressing 'Run now'.

More Help

Antivirus Scheduler

Since the scanning will take some time, and works best if you have closed all other programs, it is best for you to schedule the scanning at a time when you are not using your computer and it is standing idly by. This implies that the user must previously create a so-called task, job or scan event.

The **Scheduler** contains a wizard for creating new scan tasks. This will assist you any time you need to do any operation with these scan events, no matter if it's creating a new task or modifying an existing one.

The **Scheduler** section contains some buttons for administrating the scan tasks.

- **New** - launches the wizard that will guide you through the creation of a new scan task.
- **Modify** - modifies the properties of a previously created task. It also launches the wizard.

Note

If you modify the event's name, a new event will be created, under the newly introduced name.

- **Delete** - deletes a selected task.
- **Properties** - opens the properties of the selected task.
- **Run Now** - runs the selected task.

The Scheduler's screen also contains a list where all the scan tasks can be seen, with their names, the date of the first execution, the date of the next execution and the task's type (periodically or one time only).

If you right-click a scheduled event, a contextual menu with options similar to those described above will appear.

Note

The **Scheduler** allows an unlimited number of scheduled scan events.

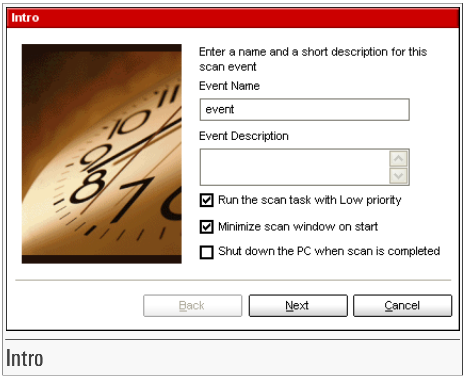
You can also navigate through the scan events using the keyboard: press the **Delete** button to erase the selected scan event, press the **Enter** button in order to view the selected event properties or press the **Insert** button in order to create a new event (the wizard will appear).

Note

Press the navigation buttons in order to scroll the page up or down or right to left.

Click **New** to set up a new entry in the scheduler. This will launch the scheduler wizard, which step by step will allow you to define your scan.

Step 1/9 - Welcome Window



Enter a name and a short description for this scan event

Event Name: event

Event Description:

☑ Run the scan task with Low priority

☑ Minimize scan window on start

□ Shut down the PC when scan is completed

Intro

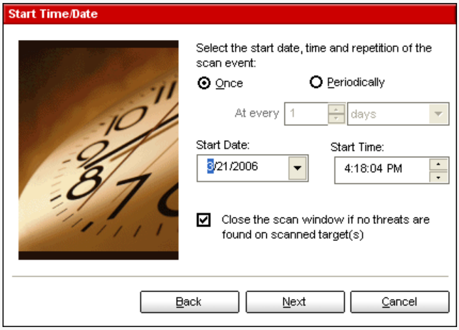
Type in the name of the new event in the **Event name** field and a short description in the **Event description** field.

The following options are available:

- **Run the task with Low priority** - Decreases the priority of the scan process. You will allow other programs to run faster and increase the time needed for the scan process to finish.
- **Minimize scan window on start** - Minimizes the scan window to system tray. Double-click the BitDefender icon to open it.
- **Shut down the PC when scan is completed** - Shut down the computer after the scan process has finished.

Click **Next** to continue. If you click **Cancel** a window will appear requesting you to confirm your option: to abort the wizard or to continue.

Step 2/9 - Start Time/Date


Start Time/Date

Select the start date, time and repetition of the scan event:

● Once ○ Periodically

At every 1 days

Start Date: 3/21/2006

Start Time: 4:18:04 PM

☑ Close the scan window if no threats are found on scanned target(s)

Start Time/Date

Select the scan frequency:

- **Once** - launches the scan only once, at a certain moment.
- **Periodically** - launches the scan periodically, at certain time intervals(hours, days, weeks, months, years) starting with a specified date and time.

If you want the scan to be repeated after certain intervals, select the checkbox corresponding to **Periodically** and type in the **At every** edit box the number of minutes/hours/days/weeks/months/years you want to repeat this process.

Note

Use the up/down arrows of this box in order to increase/decrease the number of minutes/hours/days/weeks/months/years.

Select the time interval - minutes, hours, days, weeks, months, years - to which the scan be repeated.

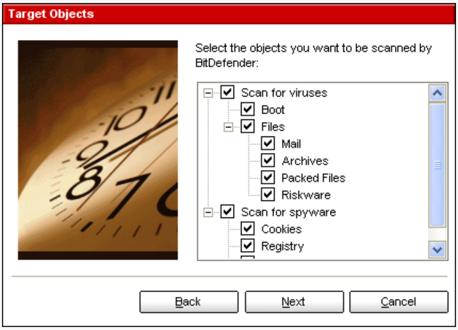
Important

If you made your option for a repeated scan, the event will be launched for an unlimited time-period. In order to give up the event, it must be erased from the events list of the Scheduler window.

If you want to automatically close the scan window if no infected or suspected files were found during the scan process, select the checkbox corresponding to this option.

Click **Back** to go to the previous step or click **Next** to continue the wizard.

Step 3/9 - Target Objects



Target Objects

Select the objects you want to be scanned by BitDefender:

- ☑ Scan for viruses
  - ☑ Boot
  - ☑ Files
    - ☑ Mail
    - ☑ Archives
    - ☑ Packed Files
    - ☑ Riskware
- ☑ Scan for spyware
  - ☑ Cookies
  - ☑ Registry

Target Objects

Select the objects you want to be scanned. The scan target is divided into two categories:

- **Scan for viruses** - scans for viruses.

Note

Select the corresponding check box in order to set the virus scan target.

The following options are available:

Option		Description
Boot		Scans the system's boot sector in order to identify the boot viruses.
Files		Scans files.
	Mail	Scans inside mail archives in order to detect infected attachments.
	Archives	Scans inside archives.
	Packed Files	Scans packed files.
	Riskware	Scans for threats other than viruses, such as dialers and adware. These files will be treated as infected files.

- **Scan for spyware** - scans for spyware applications.

Note
Select the corresponding check box in order to set the spyware scan target.

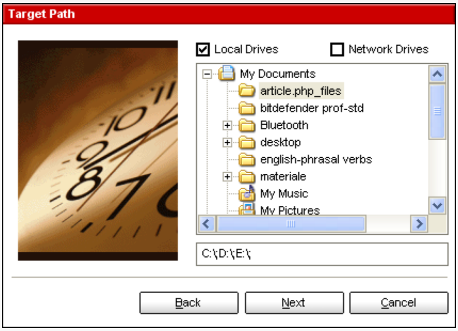
The following options are available:

Option	Description
Cookies	Scans cookie files.
Registry	Scans registry entries.
Memory	Scans memory.

To enable/disable a scan target select/clear the corresponding check box.

Click **Back** to go to the previous step or click **Next** to continue the wizard.

Step 4/9 - Target Path



Target Path

☑ Local Drives □ Network Drives

C:\D:\E:\

Target Path

Specify the path to the objects that will be scanned. This step is necessary if you have selected to scan files in the third step.

This screen is actually an exploring window that lets you select the partitions and folders to be scanned. When the cursor is placed on a folder, the complete path to the folder will appear in the field placed under this exploring window.

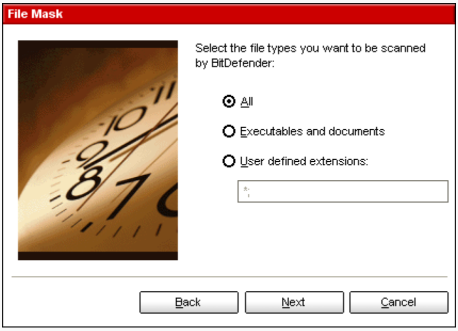
Note
Click the box with "+" to open an option or the box with "-" to close an option.

Also, in order to select the locations to be scanned, you can use the fast-selection options placed on the topside of the window:

- **Local drives** - scans all local drives;
- **Network drives** - scans all network drives.

Click **Back** to go to the previous step or click **Next** to continue the wizard.

Step 5/9 - File Mask


File Mask

Select the file types you want to be scanned by BitDefender:

● All
○ Executables and documents
○ User defined extensions:

*;

File Mask

Specify the types of the files that will be scanned. This step is necessary if you have selected to scan files in the third step.

The following options are available:

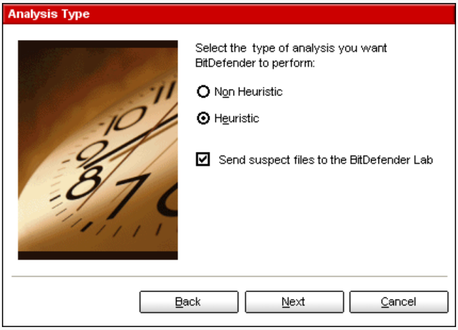
- **All** - scans all files, no matter what their type is;
- **Executables and documents** - scans only the program files and documents;
- **User defined extensions** - scans only the files whose extensions are defined by the user in the list.

Note

These extensions must be separated by a semicolon “;”.

Click **Back** to go to the previous step or click **Next** to continue the wizard.

Step 6/9 - Analysis Type



Analysis Type

Select the type of analysis you want BitDefender to perform:

○ Non Heuristic

● Heuristic

☑ Send suspect files to the BitDefender Lab

Analysis Type

Select the scan type:

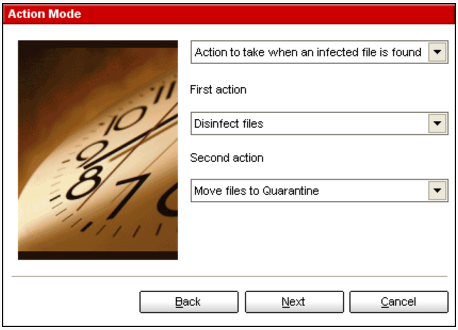
- **Non Heuristic** - means scanning the files with the procedure based on known virus signatures;
- **Heuristic** - represents a method based on certain algorithms, whose aim is to identify new unknown viruses. Occasionally, it may report a suspicious code in normal programs, generating the so-called "false positive".

You have the following option:

- **Send suspect files to the BitDefender Lab** - You will be prompted to submit all suspect files to BitDefender lab after the scan process has finished.

Click **Back** to go to the previous step or click **Next** to continue the wizard.

Step 7/9 - Action Mode



Action to take when an infected file is found

First action: Disinfect files

Second action: Move files to Quarantine

Action Mode

BitDefender allows selecting two actions in case an infected or a suspected file is found. Select the actions for infected and suspected files.

Action	Description
None (log objects)	No action will be taken on infected files. These files will appear in the report file.
Prompt user for action	When an infected file is detected, a window will appear prompting the user to select the action on that file. Depending on the importance of that file, you can select to disinfect it, isolate it in the quarantine zone or delete it.
Disinfect files	Disinfects the infected file.
Delete files	Deletes the infected files immediately, without any warning.
Rename files	Changes the extension of the infected files. The new extension of the infected files will be `.vir`. By renaming the infected files, the possibility of executing and thus of spreading the infection is removed. At the same time they can be saved for further examination and analysis.
Copy files to quarantine	Copies the infected files into the quarantine. This means practically duplicating the infected file and the copy of this file will appear in the quarantine, but the infected file will not be moved from the initial location.

Action	Description
Move files to quarantine	Moves the infected files into the quarantine zone. When the virus is in quarantine it can't do any harm.

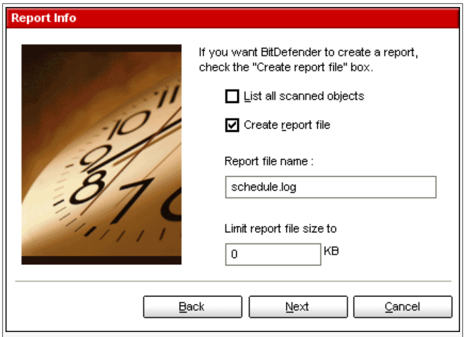
Note

We recommend you to select the first action **Disinfect files** and the second action **Move to quarantine**.

The same actions as for infected files are available for suspected ones.

Click **Back** to go to the previous step or click **Next** to continue the wizard.

Step 8/9 - Report Info



Report Info

If you want BitDefender to create a report, check the "Create report file" box.

☐ List all scanned objects

☑ Create report file

Report file name : schedule.log

Limit report file size to 0 KB

Action Mode

To create a scan report, check **Create report file**. At this moment all the other options for the creation of a report file will be enabled.

Type the name of the report file in the **Report file name** field. By default, its name is `schedule.log`. It will contain all the information about the scan process: the number of identified viruses, the number of scanned files, the number of disinfected and deleted files.

You can also limit the size of the report file. Type in the maximum file size in the corresponding field.

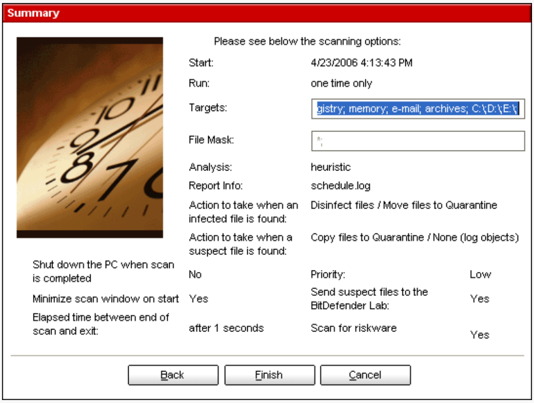
If you wish to see the information about all the scanned files, infected or not, select the option **List all scanned files**. With this option checked, the computer will slow down.

Note

The report files can be seen in the Report section from the **Antivirus** module.

Click **Back** to go to the previous step or click **Next** to continue the wizard.

Step 9/9 - Summary



Summary

Please see below the scanning options:

Start:	4/23/2006 4:13:43 PM
Run:	one time only
Targets:	gistry; memory; e-mail; archives; C:\;D:\;E:\;
File Mask:	*;
Analysis:	heuristic
Report Info:	schedule.log
Action to take when an infected file is found:	Disinfect files / Move files to Quarantine
Action to take when a suspect file is found:	Copy files to Quarantine / None (log objects)

Shut down the PC when scan is completed	No	Priority:	Low
Minimize scan window on start	Yes	Send suspect files to the BitDefender Lab:	Yes
Elapsed time between end of scan and exit:	after 1 seconds	Scan for riskware	Yes

Summary

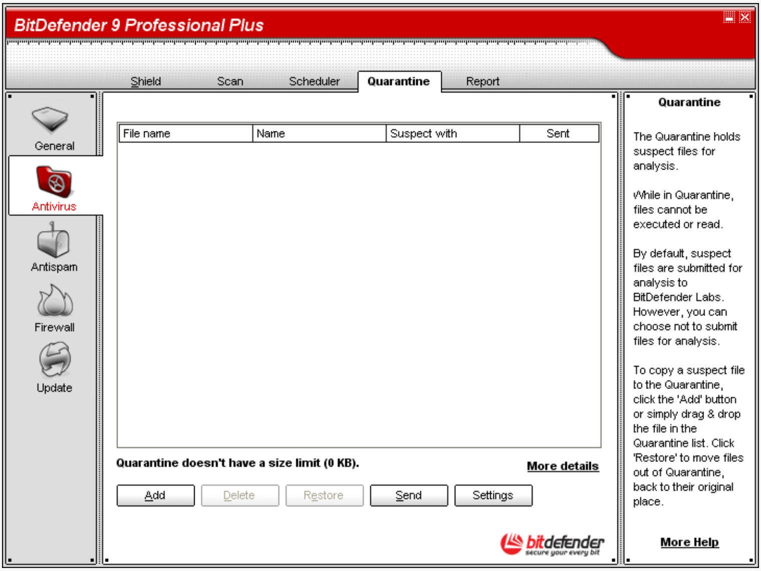
This is the last step of the wizard. In this window you can view all the settings for the new scan event and you can make any changes, by returning to the previous steps (**Back**).

If you do not want to make any modifications, click **Finish**.

The new event will appear in the Scheduler section.

7.3. Quarantine

To access this section click **Quarantine** tab from the **Antivirus** module.



Quarantine doesn't have a size limit (0 KB).

Quarantine

The Quarantine holds suspect files for analysis.

While in Quarantine, files cannot be executed or read.

By default, suspect files are submitted for analysis to BitDefender Labs. However, you can choose not to submit files for analysis.

To copy a suspect file to the Quarantine, click the 'Add' button or simply drag & drop the file in the Quarantine list. Click 'Restore' to move files out of Quarantine, back to their original place.

Quarantine

BitDefender allows isolating the infected or suspicious files in a secure area, named quarantine. By isolating these files in the quarantine, the risk of getting infected disappears and, at the same time, you have the possibility to send these files for further analysis to the BitDefender lab.

The component that ensures the administration of the isolated files is **Quarantine**. This module was designed with a function for automatically sending the infected files to the BitDefender lab.

As you may notice, the **Quarantine** section contains a list of all the files that have been isolated so far. Every file has enclosed its name, size, isolating date and submission date. If you want to see more information about the quarantined files click **More info**.

Note

When the virus is in quarantine it can't do any harm, because they cannot be executed or read.

The **Quarantine** section contains some buttons for administrating these files.

- **Add** - adds files to quarantine. Use this button to quarantine a file you suspect of being infected. A window will open and you can select the file from its location on the disk. This way the file is copied to quarantine.

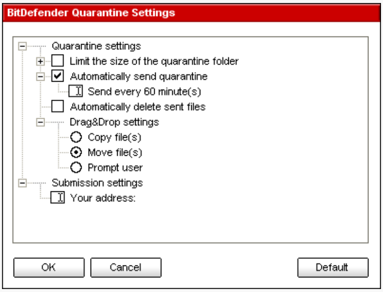
  If you want to move the file in the quarantine zone you must select the checkbox corresponding to **Delete from original location**. A quicker method to add suspicious files to the quarantine is to drag&drop them in the quarantine list.

- **Delete** - deletes the selected file from your computer.
- **Restore** - returns the selected file to its original location.
- **Send** - sends the selected files for further analysis to the BitDefender lab.

Important

You must specify some information before you may submit these files. For that click **Settings** and complete the fields from the **Submission settings** section, as described below.

- **Settings** - opens the advanced options for the quarantine zone. The following window will appear:



BitDefender Quarantine Settings

- Quarantine settings
  - □ Limit the size of the quarantine folder
  - ☑ Automatically send quarantine
    - Send every 60 minute(s)
  - □ Automatically delete sent files
  - Drag&Drop settings
    - ○ Copy file(s)
    - ● Move file(s)
    - ○ Prompt user
- Submission settings
  - Your address:

Quarantine Settings

The quarantine options are grouped in two categories:

- **Quarantine settings**
- **Submission settings**

Note

Click the box with "+" to open an option or the box with "-" to close an option.

Quarantine settings

- **Limit the size of quarantine folder** - maintains under control the size of the quarantine. This option is enabled by default and its size is 12000 kB. If you want to change this value type in a new one in the corresponding field. If you select the checkbox corresponding to **Automatically delete old files**, when the quarantine is full, and you add a new file, the oldest files in the quarantine will be automatically deleted in order to free space for the new added file.
- **Automatically send quarantine** - sends automatically the quarantined files to the BitDefender Labs for further analysis. You can set the time period between two consecutive sending processes in minutes in the **Send quarantine every** field.
- **Automatically delete sent files** - deletes automatically the quarantined files after sending them to the BitDefender Lab for analysis.
- **Drag&Drop settings** - if you are using the Drag&Drop method to add files to the quarantine here you can specify the action: copy, move or prompt user.

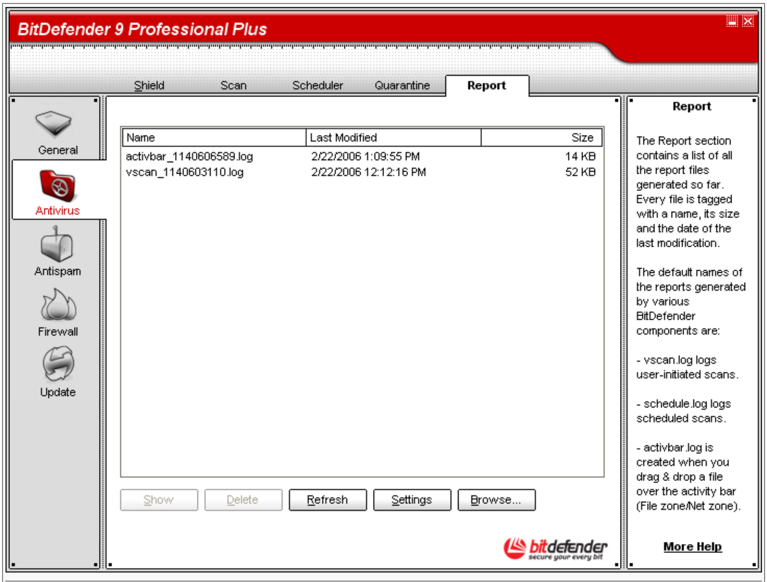
Submission settings

- **Your address** - type in your e-mail address in case you want to receive e-mail messages from our experts, regarding the suspicious files submitted for analysis.

Click **OK** to save the changes. If you click **Default** you will load the default settings.

7.4. Report

To access this section click **Report** tab from the **Antivirus** module.



Name	Last Modified	Size
activbar_1140606589.log	2/22/2006 1:09:55 PM	14 KB
vscan_1140603110.log	2/22/2006 12:12:16 PM	52 KB

Report

The Report section contains a list of all the report files generated so far. Every file is tagged with a name, its size and the date of the last modification.

The default names of the reports generated by various BitDefender components are:

- vscan.log logs user-initiated scans.

- schedule.log logs scheduled scans.

- activbar.log is created when you drag & drop a file over the activity bar (File zone/Net zone).

Report

The **Report** section contains a list of all the report files generated so far. Every file has enclosed its name, size and the date of the last modification.

When launching a scan process, the user has the possibility to opt for creating a report file where he can see information about the scan process. The user may open these reports from the management console.

BitDefender will keep track of its own activity on your computer. The default report files are the following:

- vscan.log is created when you scan your system immediately;
- schedule.log is from the scheduled scans you may have set up;
- activbar.log is created when you scan by drag&drop feature.

The **Report** section contains some buttons created for the administration of these report files. The function of each button is explained further:

- **Show** - opens the selected report file.

- **Delete** - deletes the selected report file.

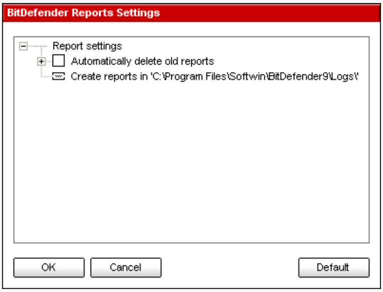
- **Refresh** - refreshes the **Report** section. If the management console is open at the **Report** section and in the meantime you perform a scan of your computer, the new report file with the scan results will be visible only after you click **Refresh**.

- **Browse** - opens a window from where you can select the report files you want to see.

Note

The report files are by default saved in the folder where BitDefender is installed. If you have saved the report files in another directory, use the **Browse** button to locate them.

- **Settings** - opens the advanced options for the report files. The following window will appear:



BitDefender Reports Settings

⊟ Report settings
⊞ □ Automatically delete old reports
Create reports in 'C:\Program Files\Softwin\BitDefender9\Logs\'

Report Settings

Note

Click the box with "+" to open an option or the box with "-" to close an option.

- **Automatically delete old reports** - maintains under control the number of the report files, by deleting those older than a specified number of days. The default time interval is 180 days. If you want to change this value type in a new one in the corresponding field.

- **Create reports in** - specifies the folder where the report files will be saved.

Click **OK** to save the changes. If you click **Default** you will load the default settings.

8. Antispam module

The **Antispam** section of this user guide contains the following topics:

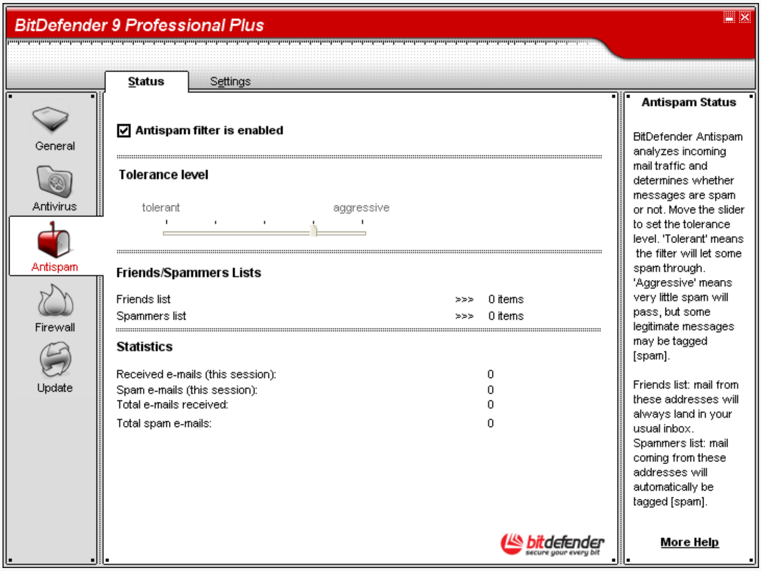
- Antispam status
- Antispam settings
- Integration with Microsoft Outlook / Outlook Express

Note

For more details regarding the **Antispam** module check the description of the "*Antispam module*" (p. 35).

8.1. Antispam status

To access this section click **Status** tab from the **Antispam** module.



☑ Antispam filter is enabled

Tolerance level

Friends/Spammers Lists

Friends list	>>>	0 items
Spammers list	>>>	0 items

Statistics

Received e-mails (this session):	0
Spam e-mails (this session):	0
Total e-mails received:	0
Total spam e-mails:	0

Antispam Status

BitDefender Antispam analyzes incoming mail traffic and determines whether messages are spam or not. Move the slider to set the tolerance level. 'Tolerant' means the filter will let some spam through. 'Aggressive' means very little spam will pass, but some legitimate messages may be tagged [spam].

Friends list: mail from these addresses will always land in your usual inbox.
Spammers list: mail coming from these addresses will automatically be tagged [spam].

Antispam status

In this section you can configure the **Antispam** module and you can view information regarding its activity.

In the **Statistics** section you can view the results of the antispam activity presented per session (since you started your computer) or a summary (since the installation of the BitDefender).

Important
To prevent spam from entering your **Inbox**, keep the **Antispam filter** enabled.

In order to configure the **Antispam** module it is necessary to proceed as follows:

8.1.1. Set the tolerance level

Move the slider to set the tolerance level.

- **Tolerant** - means the filter will let some spam through.
- **Aggressive** - means very little spam will pass, but some legitimate messages may be tagged (spam).

8.1.2. Fill in the list of addresses

The lists of addresses contain information about e-mail addresses that send you legitimate e-mail messages or spam.

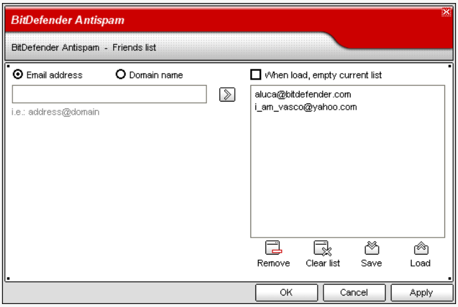
Friends list

The **Friends list** is a list of all the e-mail addresses from which you always want to receive messages, regardless of their content. Messages from your friends are not labeled as spam, even if the content resembles spam.

Note

Any mail coming from an address contained in the **Friends list**, will automatically be delivered to your Inbox without further processing.

To manage the **Friends list** click >>> (corresponding to the **Friends list**) or click the **Friends** button from the "*Antispam toolbar*" (p. 98).



aluca@bitdefender.com
i_am_vasco@yahoo.com

Friends list

Here you can add or remove entries from the **Friends list**.

If you want to add an e-mail address check the **Email address** option, type in the address and click ▷. The address will appear in the **Friends list**.

Important

Syntax: `<name@domain.com>`.

If you want to add a domain check the **Domain name** option, type in the domain and click ▷. The domain will appear in the **Friends list**.

Important
Syntax:

- `<@domain.com>`, `<*domain.com>` and `<domain.com>` - all the received e-mail messages from `<domain.com>` will reach your **Inbox** regardless of their content;
- `<*domain*>` - all the received e-mail messages from `<domain>` (no matter the domain suffixes) will reach your **Inbox** regardless of their content;
- `<*com>` - all the received e-mail messages having the domain suffix `<com>` will reach your **Inbox** regardless of their content;

To delete an item from the list, select it and click **Remove** button.

If you click **Clear list** button you will delete all entries from the list, but notice: it is impossible to recover them.

Use the **Save**/ **Load** buttons to save / load the **Friends list** to a desired location. The file will have `.bwl` extension.

Note
We recommend that you add your friends' names and e-mail addresses to the **Friends list**. BitDefender does not block messages from those on the list; therefore, adding friends helps ensure that legitimate messages get through.

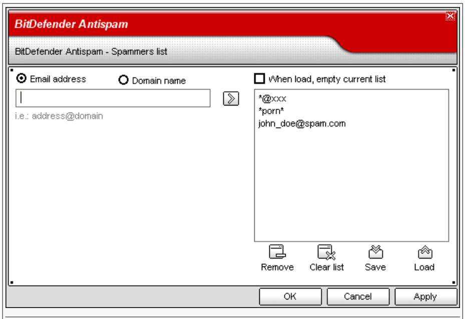
Click **Apply** and **OK** to save and close the **Friends list**.

Spammers list

The **Spammers list** is a list of all the e-mail addresses from which you don't want to receive messages, regardless of their content.

Note
Any e-mail message received from an address contained in the **Spammers list** will be automatically marked as SPAM, without further processing.

To manage the **Spammers list** click **>>>** (corresponding to the **Spammers list**) or click the **Spammers** button from the "*Antispam toolbar*" (p. 98).



*@xxx
porn
john_doe@spam.com

Spammers list

Here you can add or remove entries from the **Spammers list**.

If you want to add an e-mail address check the **Email address** option, type in the address and click ⊳ . The address will appear in the **Spammers list**.

Important

Syntax: `<name@domain.com>`.

If you want to add a domain check the **Domain name** option, type in the domain and click ⊳ . The domain will appear in the **Spammers list**.

Important

Syntax:

- `<@domain.com>`, `<*domain.com>` and `<domain.com>` - all the received e-mail messages from `<domain.com>` will be tagged as SPAM;
- `<*domain*>` - all the received e-mail messages from `<domain>` (no matter the domain suffixes) will be tagged as SPAM;
- `<*com>` - all the received e-mail messages having the domain suffix `<com>` will be tagged as SPAM.

To delete an item from the list, select it and click the **Remove** button.

If you click the **Clear list** button you will delete all entries from the list, but notice: it is impossible to recover them.

Use the Save/ Load buttons to save / load the **Spammers list** to a desired location. The file will have `.bwl` extension.

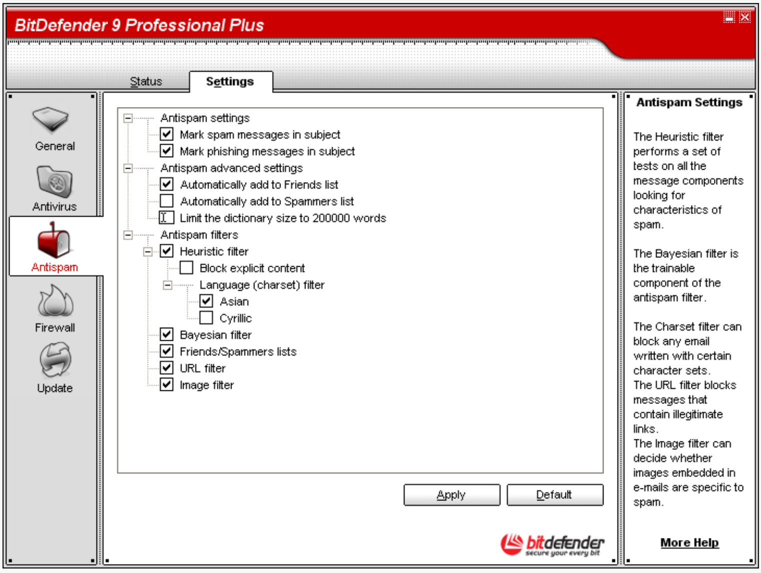
Click **Apply** and **OK** to save and close the **Spammers list**.

Important

If you want to reinstall BitDefender it's a good idea to save the **Friends** / **Spammers** lists before, and after the reinstallation process is over you may load them.

8.2. Antispam settings

To access this section click **Settings** tab from the **Antispam** module.



- Antispam settings
  - ☑ Mark spam messages in subject
  - ☑ Mark phishing messages in subject
- Antispam advanced settings
  - ☑ Automatically add to Friends list
  - □ Automatically add to Spammers list
  - □ Limit the dictionary size to 200000 words
- Antispam filters
  - ☑ Heuristic filter
    - □ Block explicit content
    - Language (charset) filter
      - ☑ Asian
      - □ Cyrillic
  - ☑ Bayesian filter
  - ☑ Friends/Spammers lists
  - ☑ URL filter
  - ☑ Image filter

Antispam Settings

The Heuristic filter performs a set of tests on all the message components looking for characteristics of spam.

The Bayesian filter is the trainable component of the antispam filter.

The Charset filter can block any email written with certain character sets.
The URL filter blocks messages that contain illegitimate links.
The Image filter can decide whether images embedded in e-mails are specific to spam.

Antispam settings

Here you can enable/disable each one of the Antispam filters and you can specify some other settings regarding the Antispam module.

Three categories of options are available (**Antispam settings**, **Antispam advanced settings** and **Antispam filters**) organized like an expandable menu, similar to those from Windows.

Note

Click the box labeled "+" to open a category or click the one labeled "-" to close it.

8.2.1. Antispam settings

- **Mark spam messages in subject** - all e-mail messages considered to be spam will be tagged with SPAM in the subject line.
- **Mark phishing messages in subject** - all e-mail messages considered to be phishing messages will be tagged with SPAM in the subject line.

8.2.2. Antispam advanced settings

- **Automatically add to Friends list** - the next time you click ✓ **Not Spam** button from the "*Antispam toolbar*" (p. 98) the sender will be added automatically to the **Friends list**.
- **Automatically add to Spammers list** - the next time you click ✗ **Is Spam** button from the "*Antispam toolbar*" (p. 98) the sender will be added automatically to the **Spammers list**.

  Note

  The ✓ **Not Spam** and the ✗ **Is Spam** buttons are used to train the Bayesian filter.

- **Limit the dictionary size to 200000 words** - sets the size of the Bayesian dictionary - smaller is faster, bigger is more accurate.

  Note

  The recommended size is: 200.000 words.

8.2.3. Antispam filters

- **Heuristic filter** - activates/deactivates the Heuristic filter;
- **Block explicit content** - activates/deactivates the detection of messages with SEXUALLY EXPLICIT in the subject line;

- **Language (charset) filter** - opens the Charset filter from where you can select to block messages written in Cyrillic and/or Asian charsets;
- **Bayesian filter** - activates/deactivates the Bayesian filter;
- **Friends/Spammers lists** - activates/deactivates the Friends/Spammers lists;
- **URL filter** - activates/deactivates the URL filter;
- **Image filter** - activates/deactivates the Image filter.

Note
To activate/deactivate a filter select/clear the checkbox corresponding to it.

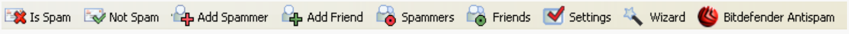
Click **Apply** to save the changes or click **Default** to load the default settings.

8.3. Integration with Microsoft Outlook / Outlook Express

BitDefender integrates directly with Microsoft Outlook / Outlook Express through an intuitive and easy-to-use toolbar.

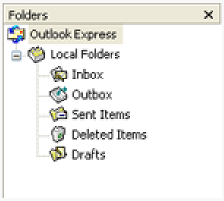
8.3.1. Antispam toolbar

At the topside of Microsoft Outlook / Outlook Express you can see the Antispam toolbar.



Antispam toolbar

Important
The difference between BitDefender Antispam for Microsoft Outlook or Outlook Express is that the SPAM messages are moved in the **Spam** folder for Microsoft Outlook while for Outlook Express they are moved in the **Deleted Items** folder. In both cases the messages are tagged as SPAM in the subject line.



Spam folder

The **Spam** folder is created automatically by BitDefender in Microsoft Outlook and is listed at the same level with the items from the **Folder list**(Calendar, Contacts, etc).

Each button from the BitDefender toolbar will be explained below:

- **Is Spam** - sends a message to the Bayesian module indicating that the selected e-mail is spam. The e-mail will be tagged as SPAM and moved to the **Spam** folder.

  The future e-mail messages that fit the same patterns will be tagged as SPAM.

  Note
  You can select one e-mail or as many e-mail messages as you want.

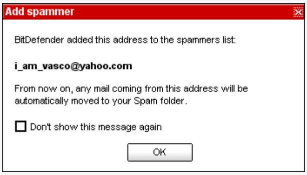
- **Not Spam** - sends a message to the Bayesian module indicating that the selected e-mail is not spam BitDefender shouldn't have tagged it. The e-mail will be moved from the **Spam** folder to the **Inbox** directory.

  The future e-mail messages that fit the same patterns will no longer be tagged as SPAM.

  Note
  You can select one e-mail or as many e-mail messages as you want.

  Important
  The **Not Spam** button becomes active when you select a message marked as SPAM by BitDefender (normally these messages are located in the **Spam** folder).

- **Add spammer** - adds the sender of the selected e-mail to the **Spammers list**.



Add spammer

BitDefender added this address to the spammers list:

i_am_vasco@yahoo.com

From now on, any mail coming from this address will be automatically moved to your Spam folder.

□ Don't show this message again

Add spammer

Select **Don't show this message again** if you don't want to be prompted for confirmation when you add a spammer's address to the list.

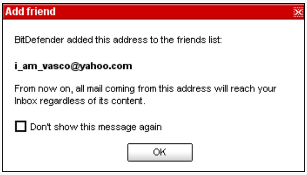
Click **OK** to close the window.

The future e-mail messages from that address will be tagged as SPAM.

Note

You can select one sender or as many senders as you want.

- **Add friend** - adds the sender of the selected e-mail to the **Friends list**.



Add friend

BitDefender added this address to the friends list:

i_am_vasco@yahoo.com

From now on, all mail coming from this address will reach your Inbox regardless of its content.

□ Don't show this message again

Add friend

Select **Don't show this message again** if you don't want to be prompted for confirmation when you add a friend's address to the list.

Click **OK** to close the window.

You will always receive e-mail messages from this address no matter what they contain.

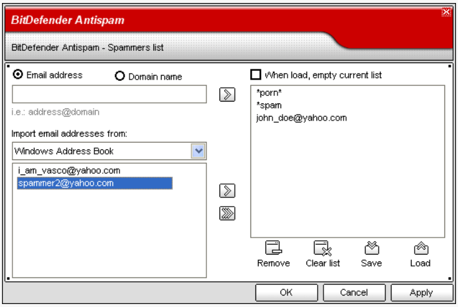
Note

You can select one sender or as many senders as you want.

- **Spammers** - opens the **Spammers list** that contains all the e-mail addresses from which you don't want to receive messages, regardless of their content.

Note

Any e-mail message received from an address contained in the **Spammers list** will be automatically marked as SPAM, without further processing.



● Email address ○ Domain name

□ When load, empty current list

porn
*spam
john_doe@yahoo.com

Import email addresses from: Windows Address Book

i_am_vasco@yahoo.com
spammer2@yahoo.com

Spammers list

Here you can add or remove entries from the **Spammers list**.

If you want to add an e-mail address check the **Email address** option, type in the address and click the ▷ button. The address will appear in the **Spammers list**.

Important

Syntax: `<name@domain.com>`.

If you want to add a domain check the **Domain name** option, type in the domain and click the ▷ button. The domain will appear in the **Spammers list**.

Important

Syntax:

- `<@domain.com>`, `<*domain.com>` and `<domain.com>` - all the received e-mail messages from `<domain.com>` will be tagged as SPAM;
- `<*domain*>` - all the received e-mail messages from `<domain>` (no matter the domain suffixes) will be tagged as SPAM;
- `<*com>` - all the received e-mail messages having the domain suffix `<com>` will be tagged as SPAM.

From the **Import email addresses from** drop-down menu select **Windows Address Book**/**Outlook Express Folders** to import e-mail addresses from **Microsoft Outlook**/**Outlook Express**.

For **Microsoft Outlook Express** a new window will appear from where you can select the folder that contains the e-mail addresses you want to add to the **Spammers list**. Choose them and click **Select**.

In both cases the e-mail addresses will appear in the import list. Select the desired ones and click ▷ to add them to the **Spammers list**. If you click » all the e-mail addresses will be added to the list.

To delete an item from the list, select it and click the **Remove** button.

If you click the **Clear list** button you will delete all entries from the list, but notice: it is impossible to recover them.

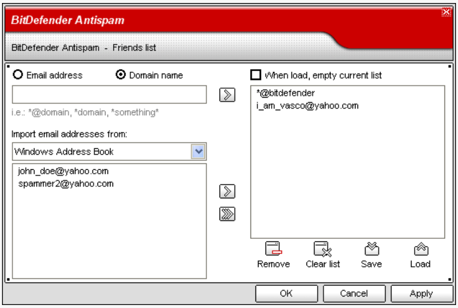
Use the **Save**/ **Load** buttons to save / load the **Spammers list** to a desired location. The file will have `.bwl` extension.

Click **Apply** and **OK** to save and close the **Spammers list**.

- **Friends** - opens the **Friends list** that contains all the e-mail addresses from which you always want to receive e-mail messages, regardless of their content.

Note

Any mail coming from an address contained in the **Friends list**, will automatically be delivered to your Inbox without further processing.



○ Email address ● Domain name

i.e.: *@domain, *domain, *something*

Import email addresses from: Windows Address Book

john_doe@yahoo.com
spammer2@yahoo.com

□ When load, empty current list

*@bitdefender
i_am_vasco@yahoo.com

Friends list

Here you can add or remove entries from the **Friends list**. If you want to add an e-mail address check the **Email address** option, type in the address and click the ▷ button. The address will appear in the **Friends list**.

Important

Syntax: `<name@domain.com>`.

If you want to add a domain check the **Domain name** option, type in the domain and click the ▷ button. The domain will appear in the **Friends list**.

Important

Syntax:

- `<@domain.com>`, `<*domain.com>` and `<domain.com>` - all the received e-mail messages from `<domain.com>` will reach your **Inbox** regardless of their content;
- `<*domain*>` - all the received e-mail messages from `<domain>` (no matter the domain suffixes) will reach your **Inbox** regardless of their content;
- `<*com>` - all the received e-mail messages having the domain suffix `<com>` will reach your **Inbox** regardless of their content;

From the **Import email addresses from** drop-down menu select **Windows Address Book**/**Outlook Express Folders** to import e-mail addresses from **Microsoft Outlook**/**Outlook Express**.

For **Microsoft Outlook Express** a new window will appear from where you can select the folder that contains the e-mail addresses you want to add to the **Friends list**. Choose them and click **Select**.

In both cases the e-mail addresses will appear in the import list. Select the desired ones and click ▷ to add them to the **Friends list**. If you click ▷▷ all the e-mail addresses will be added to the list.

To delete an item from the list, select it and click the **Remove** button.

If you click the **Clear list** button you will delete all entries from the **Friends list**, but notice: it is impossible to recover them.

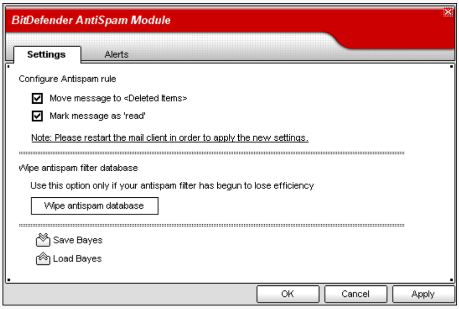
Use the **Save**/ **Load** buttons to save / load the **Friends list** to a desired location. The file will have `.bwl` extension.

Note

We recommend that you add your friends' names and e-mail addresses to the **Friends list**. BitDefender does not block messages from those on the list; therefore, adding friends helps ensure that legitimate messages get through.

Click **Apply** and **OK** to save and close the **Friends list**.

- ☑ **Settings** - opens the **Settings** window where you can specify some options for the **Antispam** module.



Configure Antispam rule

☑ Move message to <Deleted Items>

☑ Mark message as 'read'

Note: Please restart the mail client in order to apply the new settings.

Wipe antispam filter database

Use this option only if your antispam filter has begun to lose efficiency

Settings

The following options are available:

- **Move message to Deleted Items** - moves the spam messages to the **Deleted Items** (only for Microsoft Outlook Express);
- **Mark message as 'read'** - marks all the spam messages as read so as not to be disturbing when new spam messages arrive.

If your antispam filter is very inaccurate, you may need to wipe the filter database and retrain the Bayesian filter. Click **Wipe antispam database** to reset the Bayesian database.

Use the **Save Bayes**/ **Load Bayes** buttons to save / load the Bayesian database list to a desired location. The file will have `.dat` extension.

Click the **Alerts** tab if you want to access the section where you can disable the apparition of the confirmation windows for the **Add spammer** and **Add friend** buttons.

- **Wizard** - opens the wizard that will step you through the process of training the Bayesian filter, so that the efficiency of BitDefender Antispam will be further increased. You can also add addresses from your **Address Book** to your **Friends list** / **Spammers list**.
- **BitDefender Antispam** - opens the Management Console.

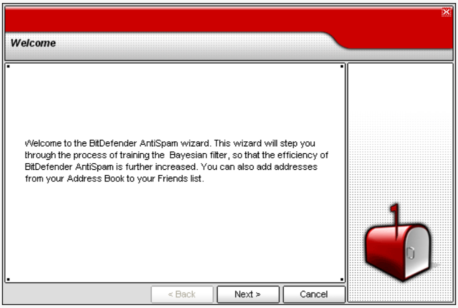
8.3.2. Antispam configuration wizard

The first time you run Microsoft Outlook / Outlook Express with BitDefender installed, a wizard will appear helping you to configure the Friends list and the Spammers list and to train the Bayesian filter in order to increase the efficiency of the Antispam filters.

Note

The wizard can also be launched any time you want by clicking the **Wizard** button from the *"Antispam toolbar"* (p. 98).

Step 1/6 - Welcome window



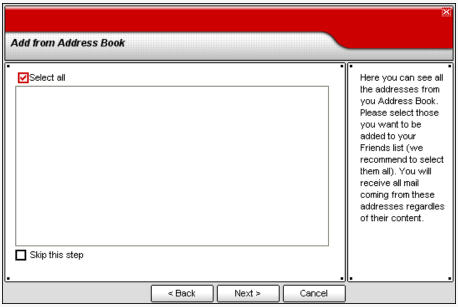
Welcome

Welcome to the BitDefender AntiSpam wizard. This wizard will step you through the process of training the Bayesian filter, so that the efficiency of BitDefender AntiSpam is further increased. You can also add addresses from your Address Book to your Friends list.

Welcome window

Click **Next**.

Step 2/6 - Fill in the Friends list



Add from Address Book

☑ Select all

□ Skip this step

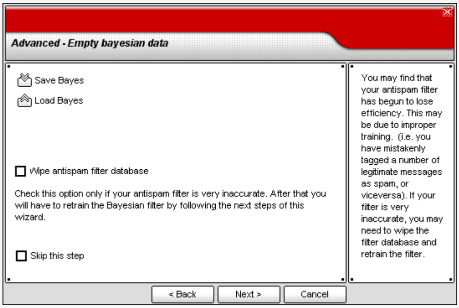
Here you can see all the addresses from you Address Book. Please select those you want to be added to your Friends list (we recommend to select them all). You will receive all mail coming from these addresses regardles of their content.

Fill in the Friends list

Here you can see all the addresses from your **Address Book**. Please select those you want to be added to your **Friends list** (we recommend to select them all). You will receive all the e-mail messages from these addresses, regardless of their content.

Select **Skip this step** if you want to pass over this step. Click **Back** to go to the previous step or click **Next** to continue the wizard.

Step 3/6 - Delete Bayesian database



□ Wipe antispam filter database

Check this option only if your antispam filter is very inaccurate. After that you will have to retrain the Bayesian filter by following the next steps of this wizard.

□ Skip this step

You may find that your antispam filter has begun to lose efficiency. This may be due to improper training. (i.e. you have mistakenly tagged a number of legitimate messages as spam, or viceversa). If your filter is very inaccurate, you may need to wipe the filter database and retrain the filter.

Delete Bayesian database

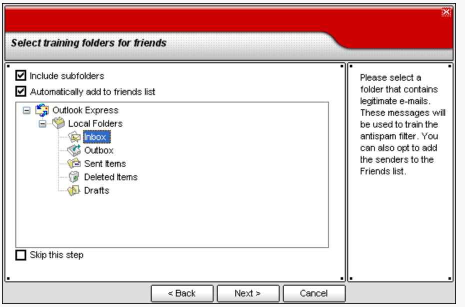
You may find that your antispam filter has begun to lose efficiency. This may be due to improper training. (i.e. you have mistakenly tagged a number of legitimate messages as spam, or vice versa). If your filter is very inaccurate, you may need to wipe the filter database and retrain the filter by following the next steps of this wizard.

Select **Wipe antispam filter database** if you want to reset the Bayesian database.

Use the **Save Bayes**/ **Load Bayes** buttons to save / load the Bayesian database list to a desired location. The file will have `.dat` extension.

Select **Skip this step** if you want to pass over this step. Click **Back** to go to the previous step or click **Next** to continue the wizard.

Step 4/6 - Train the Bayesian filter with legitimate e-mail messages


Select training folders for friends

☑ Include subfolders

☑ Automatically add to friends list

□ Skip this step

Please select a folder that contains legitimate e-mails. These messages will be used to train the antispam filter. You can also opt to add the senders to the Friends list.

Train the Bayesian filter with legitimate e-mail messages

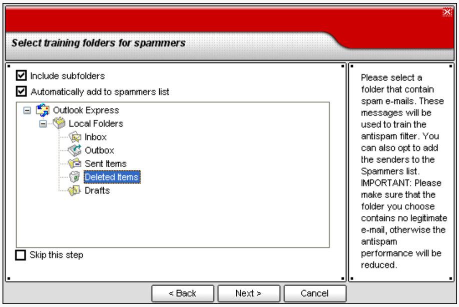
Please select a folder that contains legitimate e-mail messages. These messages will be used to train the antispam filter.

At the topside of the window 2 options are available:

- **Include subfolders** - to include the subfolders to your selection;
- **Automatically add to friends list** - to add the senders to the **Friends list**.

Select **Skip this step** if you want to pass over this step. Click **Back** to go to the previous step or click **Next** to continue the wizard.

Step 5/6 - Train the Bayesian filter with spam e-mail messages



Select training folders for spammers

☑ Include subfolders

☑ Automatically add to spammers list

- Outlook Express
  - Local Folders
    - Inbox
    - Outbox
    - Sent Items
    - Deleted Items
    - Drafts

☐ Skip this step

Please select a folder that contain spam e-mails. These messages will be used to train the antispam filter. You can also opt to add the senders to the Spammers list. IMPORTANT: Please make sure that the folder you choose contains no legitimate e-mail, otherwise the antispam performance will be reduced.

Train the Bayesian filter with spam e-mail messages

Please select a folder that contains spam e-mail messages. These messages will be used to train the antispam filter.

Important

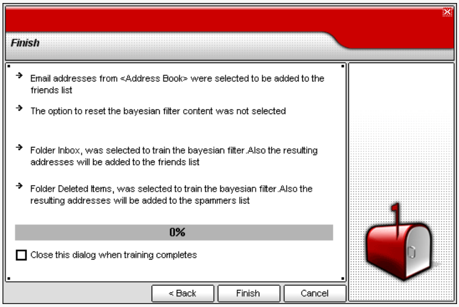
Please make sure that the folder you choose contains no legitimate e-mail at all, otherwise the antispam performance will be considerably reduced.

At the topside of the window 2 options are available:

- **Include subfolders** - to include the subfolders to your selection;
- **Automatically add to spammers list** - to add the senders to the **Spammers list**.

Select **Skip this step** if you want to pass over this step. Click **Back** to go to the previous step or click **Next** to continue the wizard.

Step 6/6 - Summary



- Email addresses from <Address Book> were selected to be added to the friends list
- The option to reset the bayesian filter content was not selected
- Folder Inbox, was selected to train the bayesian filter.Also the resulting addresses will be added to the friends list
- Folder Deleted Items, was selected to train the bayesian filter.Also the resulting addresses will be added to the spammers list

Summary

Here you can view all the settings for the configuration wizard. You can make any changes, by returning to the previous steps (click **Back**).

If you do not want to make any modifications, click **Finish** to end the wizard.

9. Firewall module

The **Firewall** section of this user guide contains the following topics:

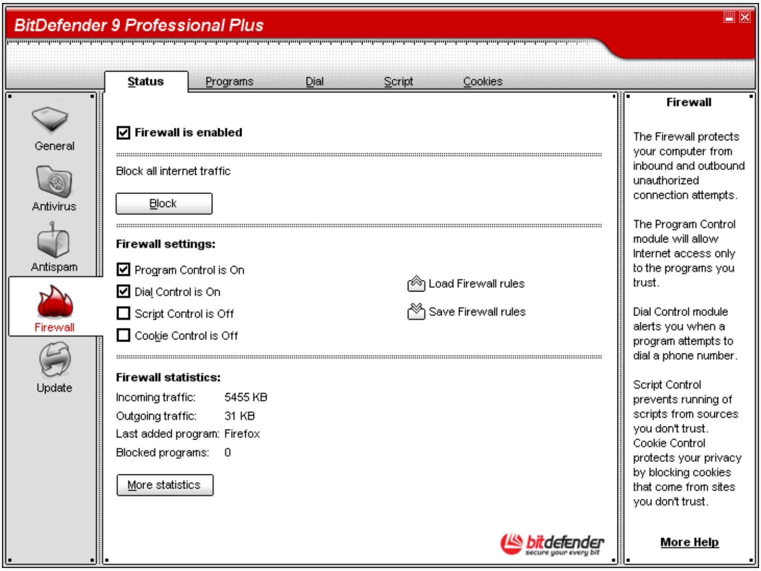
- Firewall status
- Program Control
- Dial Control
- Script Control
- Cookie Control

Note

For more details regarding the **Firewall** module check the description of the “*Firewall module*” (p. 39).

9.1. Firewall status

To access this section click **Status** tab from the **Firewall** module.



☑ **Firewall is enabled**

Block all internet traffic

Firewall settings:

☑ Program Control is On

☑ Dial Control is On

□ Script Control is Off

□ Cookie Control is Off

Firewall statistics:

Incoming traffic:	5455 KB
Outgoing traffic:	31 KB
Last added program:	Firefox
Blocked programs:	0

Firewall

The Firewall protects your computer from inbound and outbound unauthorized connection attempts.

The Program Control module will allow Internet access only to the programs you trust.

Dial Control module alerts you when a program attempts to dial a phone number.

Script Control prevents running of scripts from sources you don't trust. Cookie Control protects your privacy by blocking cookies that come from sites you don't trust.

Firewall status

The **Firewall** protects your computer from inbound and outbound unauthorized connection attempts.

Note

To be protected against Internet attacks keep the **Firewall** enabled.

In this section you can enable / disable any protection offered by the **Firewall** module (Program Control, Dial Control, Script Control and Cookie Control). A protection is enabled when the corresponding checkbox is selected.

Click **Block** to block all the Internet traffic.

Note

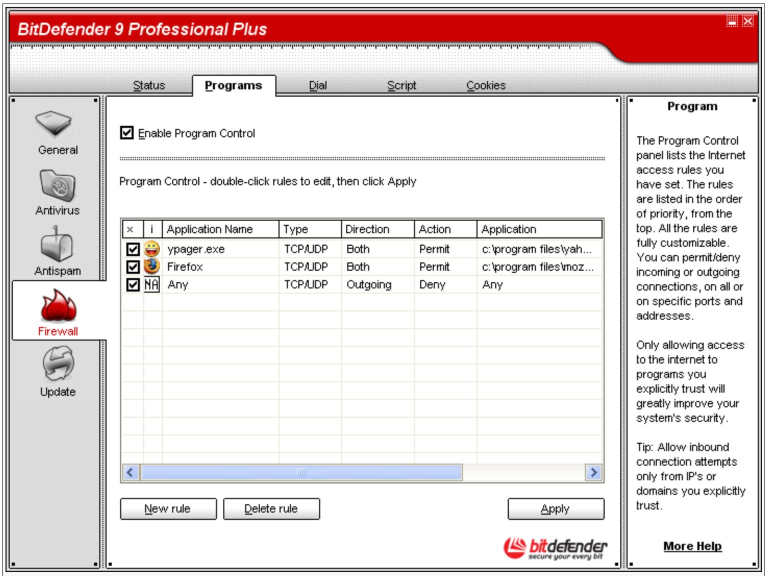
If you are not the only person using this computer, it is recommended that you protect your BitDefender settings with a password. To set a password, enter the **General** module, access the Settings section and use the **Enable password protection** option.

Use the **Save Firewall rules** / **Load Firewall rules** buttons to save / load the rules you have made for the Firewall module to a desired location. This way you can use the same rules after you reinstall or repair your BitDefender product.

In the bottom side of the section you can see the BitDefender statistics about traffic and programs. Click **More statistics** if you want to see a window with more information regarding these statistics.

9.2. Program Control

To access this section click **Programs** tab from the **Firewall** module.



☑ Enable Program Control

Program Control - double-click rules to edit, then click Apply

×	i	Application Name	Type	Direction	Action	Application
☑		ypager.exe	TCP/UDP	Both	Permit	c:\program files\yah...
☑		Firefox	TCP/UDP	Both	Permit	c:\program files\moz...
☑	NA	Any	TCP/UDP	Outgoing	Deny	Any

Program

The Program Control panel lists the Internet access rules you have set. The rules are listed in the order of priority, from the top. All the rules are fully customizable. You can permit/deny incoming or outgoing connections, on all or on specific ports and addresses.

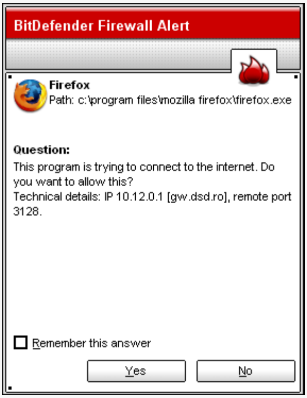
Only allowing access to the internet to programs you explicitly trust will greatly improve your system's security.

Tip: Allow inbound connection attempts only from IP's or domains you explicitly trust.

Program Control

Program Control is the most important part of your firewall. It monitors which programs are allowed to use your Internet connection. This is essential to stop Trojans.

With **Program Control** enabled, BitDefender will ask for your permission whenever a new program tries to send or receive information to or from the Internet:



BitDefender Firewall Alert

Firefox
Path: c:\program files\mozilla firefox\firefox.exe

Question:
This program is trying to connect to the internet. Do you want to allow this?
Technical details: IP 10.12.0.1 [gw.dsd.ro], remote port 3128.

□ Remember this answer

Program Control alert

You can see the following: the application that is trying to access the internet, the IP address and the port on which the application is trying to connect.

Check **Remember this answer** option and click **Yes** or **No** and a rule will be created, applied and listed in the rules table. This way you will no longer be notified when the process repeats.

Important
Allow inbound connection attempts only from IP's or domains you explicitly trust.

The rules are added to the list when you answer the questions from BitDefender about a new program that tries to access the Internet.

Every rule that has been remembered can be accessed in the **Programs** section for further fine-tuning.

Important
The rules are listed in order of their priority starting from the top, meaning the first rule has the highest priority. Drag&drop rules in order to change their priority.

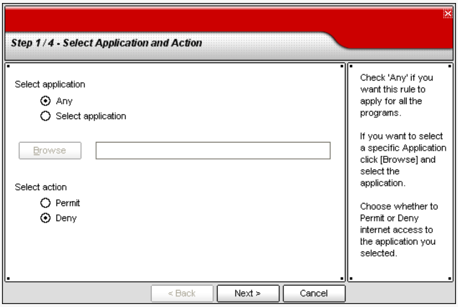
To delete a rule, just select it and click **Delete rule**. To modify a rule's attribute just double click its field. To temporarily deactivate a rule without deleting it, clear the corresponding checkbox.

The rules can be input automatically (through the alert window) or manually (click **New rule** and choose the parameters for the rule). The configuration wizard will appear.

9.2.1. Configuration wizard

The configuration wizard is a 4 steps procedure.

Step 1/4 - Select application and action



Step 1 / 4 - Select Application and Action

Select application

● Any

○ Select application

Select action

○ Permit

● Deny

Check 'Any' if you want this rule to apply for all the programs.

If you want to select a specific Application click [Browse] and select the application.

Choose whether to Permit or Deny internet access to the application you selected.

Select application and action

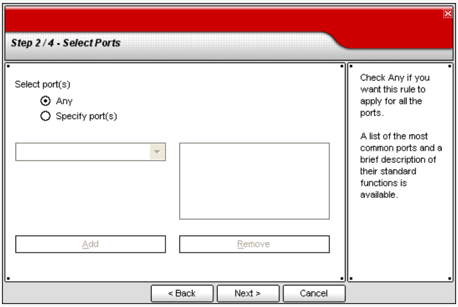
You can set the parameters:

- **Application** - select the application for the rule. You can choose only one application (click **Select application**, then **Browse** and select the application) or all the applications (just click **Any**).
- **Action** - select the action of the rule.

Action	Description
Permit	The action will be permitted.
Deny	The action will be denied.

Click **Next**.

Step 2/4 - Select ports



Step 2 / 4 - Select Ports

Select port(s)

● Any
○ Specify port(s)

Check Any if you want this rule to apply for all the ports.

A list of the most common ports and a brief description of their standard functions is available.

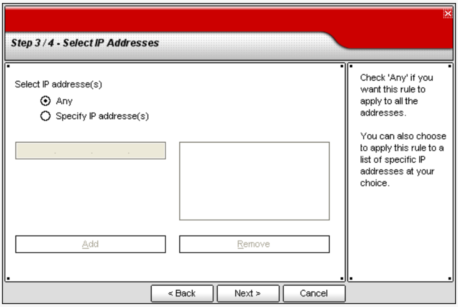
Select ports

A list with the most common ports and a brief description is available to help you select only specific ports. Click **Specify port(s)**, select the desired ports (on which the rule applies) from the corresponding drop-down menu and click **Add**.

If you click **Any** all the ports will be selected. To delete a port select it and click **Remove**.

Click **Next**.

Step 3/4 - Select IP addresses



Step 3 / 4 - Select IP Addresses

Select IP addresse(s)

● Any
○ Specify IP addresse(s)

Check 'Any' if you want this rule to apply to all the addresses.

You can also choose to apply this rule to a list of specific IP addresses at your choice.

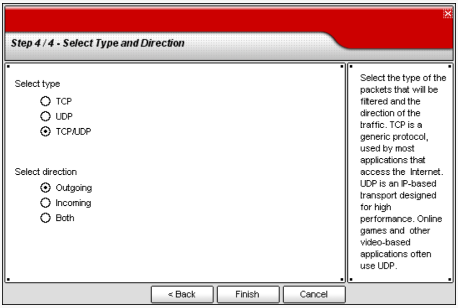
Select IP addresses

Click **Specify IP address(es)**, type in the IP addresses on which the rule will be applied and click **Add**.

Check **Any** if you want this rule to apply for any IP address. To delete an IP address select it and click **Remove**.

Click **Next**.

Step 4/4 - Select type and direction



Step 4 / 4 - Select Type and Direction

Select type

○ TCP
○ UDP
● TCP/UDP

Select direction

● Outgoing
○ Incoming
○ Both

Select the type of the packets that will be filtered and the direction of the traffic. TCP is a generic protocol, used by most applications that access the Internet. UDP is an IP-based transport designed for high performance. Online games and other video-based applications often use UDP.

Select type and direction

You can set the parameters:

- **Protocol type** - select the protocols TCP, UDP or both.

Type	Description
TCP	Transmission Control Protocol - TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.
UDP	User Datagram Protocol - UDP is an IP-based transport designed for high performance. Games and other video-based applications often use UDP.
TCP/UDP	Transmission Control Protocol and User Datagram Protocol.

- **Direction** - select the traffic direction.

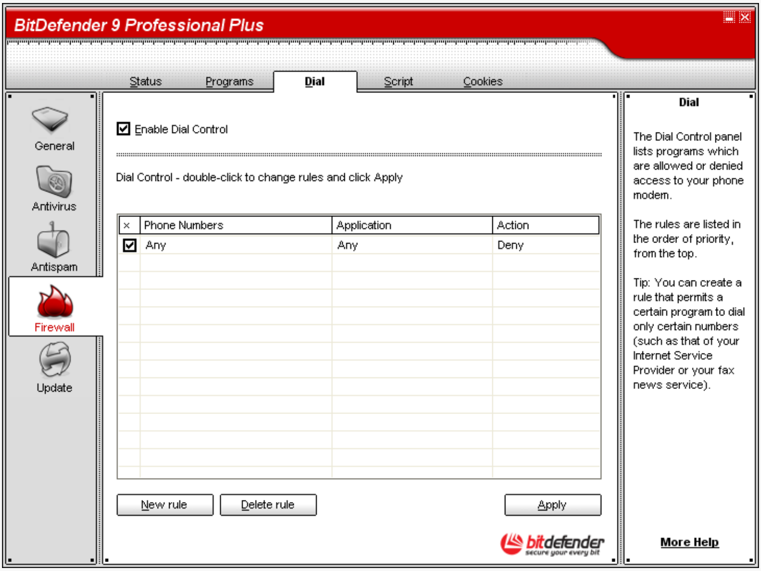
Type	Description
Outgoing	The rule applies only for the outgoing traffic.
Incoming	The rule applies only for the incoming traffic.
Both	The rule applies in both directions.

Click **Finish**.

Click **Apply** to save the changes.

9.3. Dial Control

To access this section click **Dial** tab from the **Firewall** module.



☑ Enable Dial Control

Dial Control - double-click to change rules and click Apply

×	Phone Numbers	Application	Action
☑	Any	Any	Deny

Dial

The Dial Control panel lists programs which are allowed or denied access to your phone modem.

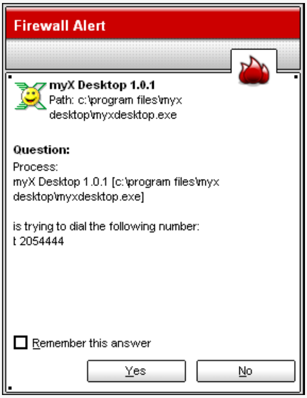
The rules are listed in the order of priority, from the top.

Tip: You can create a rule that permits a certain program to dial only certain numbers (such as that of your Internet Service Provider or your fax news service).

Dial Control

The dialers are applications that use computer's modems in order to dial different phone numbers. Usually, the dialers are used to access various locations by dialing a high-cost phone numbers.

With **Dial Control** you will be in charge of which connections to different phone numbers you permit or block. This function monitors all dialers attempting to access a computer modem, immediately warning the user and prompting him to choose whether to block or allow such operations:



Firewall Alert

myX Desktop 1.0.1
Path: c:\program files\myx desktop\myxdesktop.exe

Question:
Process:
myX Desktop 1.0.1 [c:\program files\myx desktop\myxdesktop.exe]

is trying to dial the following number:
t 2054444

□ Remember this answer

Dial Control alert

You can see the name of the application and the phone number.

Check **Remember this answer** option and click **Yes** or **No** and a rule will be created, applied and listed in the rules table. You will no longer be notified when the application tries to dial the same phone number.

Every rule that has been remembered can be accessed in the **Dial** section for further fine-tuning.

Important
The rules are listed in order of their priority starting from the top, meaning the first rule has the highest priority. Drag&drop rules in order to change their priority.

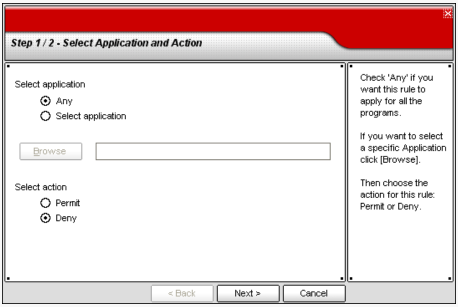
To delete a rule, just select it and click **Delete rule**. To modify a rule's attribute just double click its field. To temporarily deactivate a rule without deleting it, clear the corresponding checkbox.

The rules can be input automatically (through the alert window) or manually (click **New rule** and choose the parameters for the rule). The configuration wizard will appear.

9.3.1. Configuration wizard

The configuration wizard is a 2 steps procedure.

Step 1/2 - Select application and action



Step 1 / 2 - Select Application and Action

Select application

● Any

○ Select application

Select action

○ Permit

● Deny

Check 'Any' if you want this rule to apply for all the programs.

If you want to select a specific Application click [Browse].

Then choose the action for this rule: Permit or Deny.

Select application and action

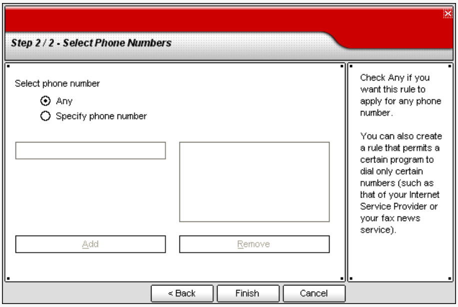
You can set the parameters:

- **Application** - select the application for the rule. You can choose only one application (click **Select application**, then **Browse** and select the application) or all the applications (just click **Any**).
- **Action** - select the action of the rule.

Action	Description
Permit	The action will be permitted.
Deny	The action will be denied.

Click **Next**.

Step 2/2 - Select the phone numbers


Step 2 / 2 - Select Phone Numbers

Select phone number

● Any
○ Specify phone number

Check Any if you want this rule to apply for any phone number.

You can also create a rule that permits a certain program to dial only certain numbers (such as that of your Internet Service Provider or your fax news service).

Select the phone numbers

Click **Specify phone number**, type in the phone number for which the rule will be applied and click **Add**.

Note

You can use wildcards in your list of banned phone number; e.g.: 1900* means all numbers beginning with 1900 will be blocked.

Check **Any** if you want this rule to apply for any phone number. To delete a phone number select it and click **Remove**.

Note

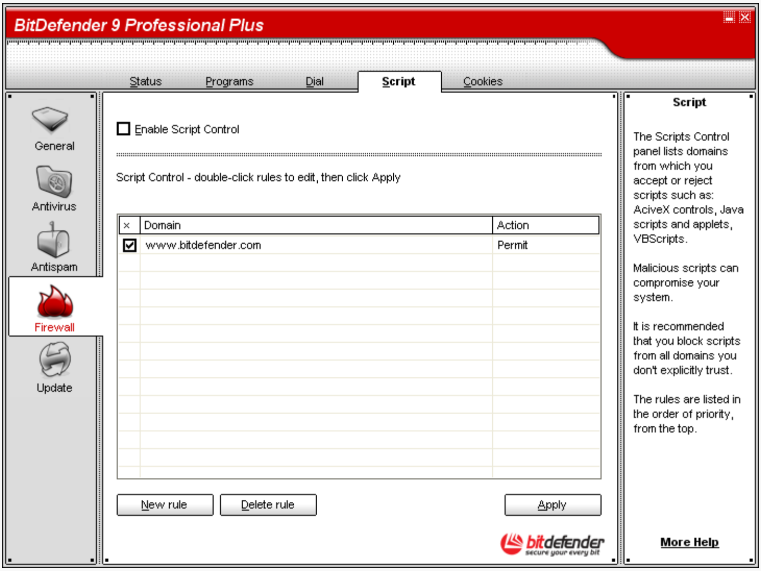
You can also create a rule that permits a certain program to dial only certain numbers (such as that of your Internet Service Provider or your fax news service).

Click **Finish**.

Click **Apply** to save the changes.

9.4. Script Control

To access this section click **Script** tab from the **Firewall** module.



☐ Enable Script Control

Script Control - double-click rules to edit, then click Apply

×	Domain	Action
☑	www.bitdefender.com	Permit

Script

The Scripts Control panel lists domains from which you accept or reject scripts such as: AciveX controls, Java scripts and applets, VBScripts.

Malicious scripts can compromise your system.

It is recommended that you block scripts from all domains you don't explicitly trust.

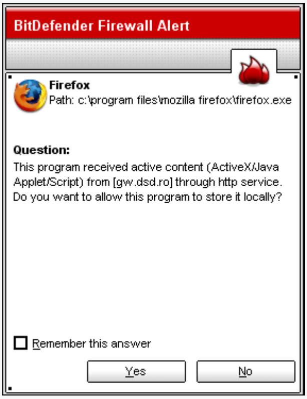
The rules are listed in the order of priority, from the top.

Script Control

Scripts and other codes such as ActiveX controls and Java applets, which are used to create interactive web pages, can be programmed to have harmful effects. ActiveX elements, for example, can gain total access to your data and they can read data from your computer, delete information, capture passwords and intercept messages while you're online. You should only accept active content from sites you fully know and trust.

BitDefender lets you choose to run these elements or to block their execution.

With **Script Control** you will be in charge of which websites you trust and which you don't. BitDefender will ask you for permission whenever a website tries to activate a script or other active content:



BitDefender Firewall Alert

Firefox
Path: c:\program files\mozilla firefox\firefox.exe

Question:
This program received active content (ActiveX/Java Applet/Script) from [gw.dsd.ro] through http service. Do you want to allow this program to store it locally?

☐ Remember this answer

Script Control alert

You can see the name of the resource.

Check **Remember this answer** option and click **Yes** or **No** and a rule will be created, applied and listed in the rules table. You will no longer be notified when the same site tries to send you active content.

Every rule that has been remembered can be accessed in the **Script** section for further fine-tuning.

Important
The rules are listed in order of their priority starting from the top, meaning the first rule has the highest priority. Drag&drop rules in order to change their priority.

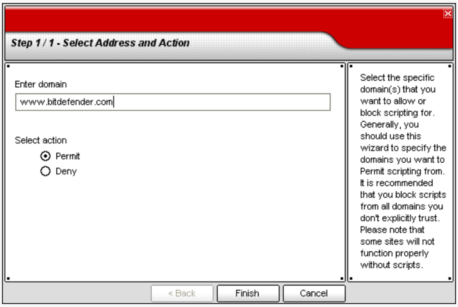
To delete a rule, just select it and click **Delete rule**. To modify a rule's attribute just double click its field. To temporarily deactivate a rule without deleting it, clear the corresponding checkbox.

The rules can be input automatically (through the alert window) or manually (click **New rule** and choose the parameters for the rule). The configuration wizard will appear.

9.4.1. Configuration wizard

The configuration wizard is a 1 step procedure.

Step 1/1 - Select address and action



Step 1 / 1 - Select Address and Action

Enter domain

www.bitdefender.com

Select action

● Permit

○ Deny

Select the specific domain(s) that you want to allow or block scripting for. Generally, you should use this wizard to specify the domains you want to Permit scripting from. It is recommended that you block scripts from all domains you don't explicitly trust. Please note that some sites will not function properly without scripts.

Select address and action

You can set the parameters:

- **Domain address** - type in the domain on which the rule should apply.
- **Action** - select the action of the rule.

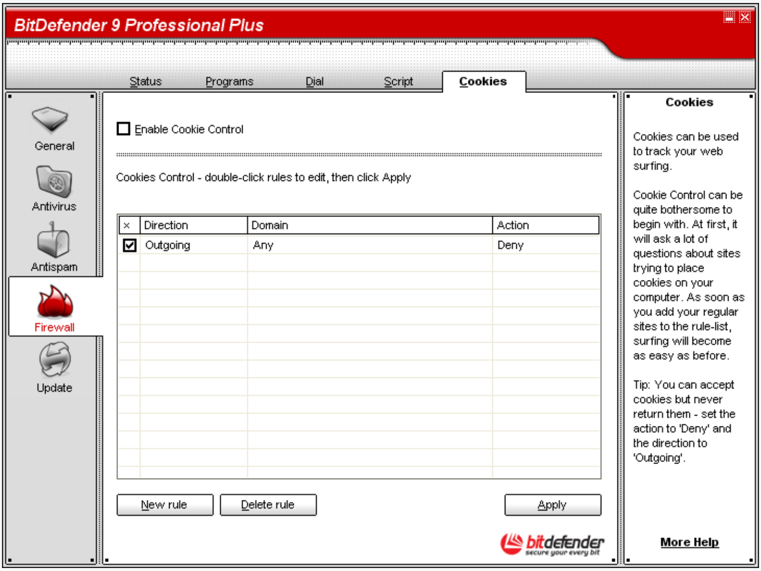
Action	Description
Permit	The scripts on that domain will execute.
Deny	The scripts on that domain will not execute.

Click **Finish**.

Click **Apply** to save the changes.

9.5. Cookie Control

To access this section click **Cookies** tab from the **Firewall** module.



□ Enable Cookie Control

Cookies Control - double-click rules to edit, then click Apply

×	Direction	Domain	Action
☑	Outgoing	Any	Deny

Cookies

Cookies can be used to track your web surfing.

Cookie Control can be quite bothersome to begin with. At first, it will ask a lot of questions about sites trying to place cookies on your computer. As soon as you add your regular sites to the rule-list, surfing will become as easy as before.

Tip: You can accept cookies but never return them - set the action to 'Deny' and the direction to 'Outgoing'.

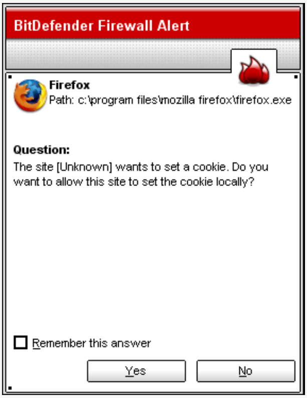
Cookie Control

Cookies are a very common occurrence on the Internet. They are small files stored on your computer. Websites create these cookies in order to keep track of specific information about you.

Cookies are generally made to make your life easier. For example they can help the website remember your name and preferences, so that you don't have to enter them on every visit.

But cookies can also be used to compromise your privacy, by tracking your surfing patterns.

This is where **Cookie Control** helps. When enabled, **Cookie Control** will ask for your permission whenever a new website tries to set a cookie:



BitDefender Firewall Alert

Firefox
Path: c:\program files\mozilla firefox\firefox.exe

Question:
The site [Unknown] wants to set a cookie. Do you want to allow this site to set the cookie locally?

□ Remember this answer

Cookie Control alert

You can see the name of the application that is trying to send the cookie file.

Check **Remember this answer** option and click **Yes** or **No** and a rule will be created, applied and listed in the rules table. You will no longer be notified the next time when you connect to the same site.

This will help you to choose which websites you trust and which you don't.

Note

Because of the great number of cookies used on the Internet today, **Cookie Control** can be quite bothersome to begin with. At first, it will ask a lot of questions about sites trying to place cookies on your computer. As soon as you add your regular sites to the rule-list, surfing will become as easy as before.

Every rule that has been remembered can be accessed in the **Cookies** section for further fine-tuning.

Important

The rules are listed in order of their priority starting from the top, meaning the first rule has the highest priority. Drag&drop rules in order to change their priority.

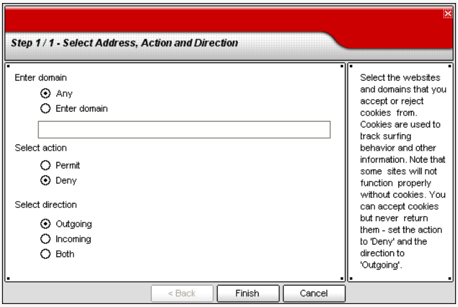
To delete a rule, just select it and click **Delete rule**. To modify a rule’s attribute just double click its field. To temporarily deactivate a rule without deleting it, clear the corresponding checkbox.

The rules can be input automatically (through the alert window) or manually (click **New rule** and choose the parameters for the rule). The configuration wizard will appear.

9.5.1. Configuration wizard

The configuration wizard is a 1 step procedure.

Step 1/1 - Select address, action and direction



Step 1 / 1 - Select Address, Action and Direction

Enter domain

● Any
○ Enter domain

Select action

○ Permit
● Deny

Select direction

● Outgoing
○ Incoming
○ Both

Select the websites and domains that you accept or reject cookies from. Cookies are used to track surfing behavior and other information. Note that some sites will not function properly without cookies. You can accept cookies but never return them - set the action to 'Deny' and the direction to 'Outgoing'.

Select address, action and direction

You can set the parameters:

- **Domain address** - type in the domain on which the rule should apply.
- **Action** - select the action of the rule.

Action	Description
Permit	The cookies on that domain will execute.
Deny	The cookies on that domain will not execute.

- **Direction** - select the traffic direction.

Type	Description
Outgoing	The rule applies only for the cookies that are sent out back to the connected site.
Incoming	The rule applies only for the cookies that are received from the connected site.
Both	The rule applies in both directions.

Click **Finish**.

Note

You can accept cookies but never return them by setting the action to **Deny** and the direction to **Outgoing**.

Click **Apply** to save the changes.

10. Update module

The **Update** section of this user guide contains the following topics:

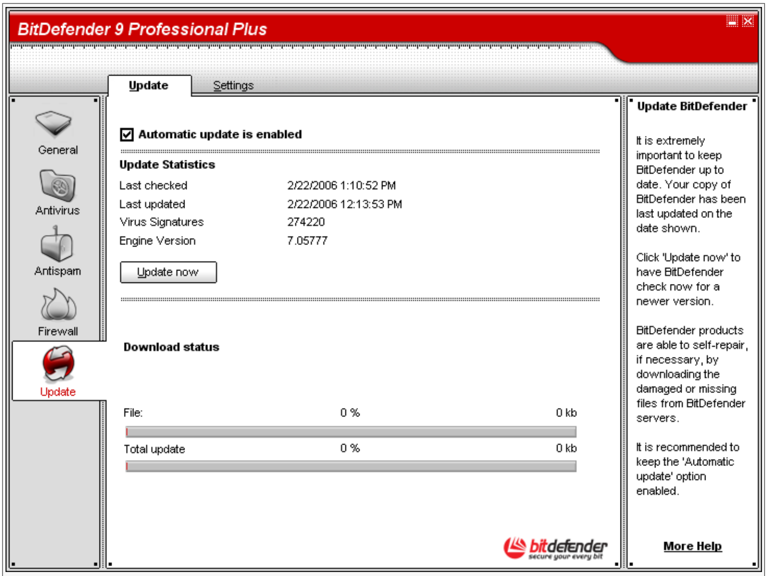
- Automatic update
- Manual update
- Update settings

Note

For more details regarding the **Update** module check the description of the "*Update module*" (p. 39).

10.1. Automatic update

To access this section click **Update** tab from the **Update** module.



☑ Automatic update is enabled

Update Statistics

Last checked	2/22/2006 1:10:52 PM
Last updated	2/22/2006 12:13:53 PM
Virus Signatures	274220
Engine Version	7.05777

Download status

File:	0 %	0 kb
Total update	0 %	0 kb

Update BitDefender

It is extremely important to keep BitDefender up to date. Your copy of BitDefender has been last updated on the date shown.

Click 'Update now' to have BitDefender check now for a newer version.

BitDefender products are able to self-repair, if necessary, by downloading the damaged or missing files from BitDefender servers.

It is recommended to keep the 'Automatic update' option enabled.

Automatic Update

If you are connected to the Internet through broadband or DSL, BitDefender takes care of this itself. It checks for updates when you turn on your computer and every **hour** after that.

If an update was detected, depending on the options set in the Automatic update options section, you will be asked to confirm the update or the update will be made automatically.

The automatic update can also be done anytime you want by clicking **Update Now**. This update is also known as **Update by user request**.

The **Update** module will connect to the BitDefender update server and will verify if any update is available. If an update was detected, depending on the options set in the Manual update settings section, you will be asked to confirm the update or the update will be made automatically.

Important

It may be necessary to restart the computer when you have completed the update. We recommend doing it as soon as possible.

Note

If you are connected to the Internet through a dial-up connection, then it's a good idea to make it a regular habit to update BitDefender by user request.

10.2. Manual update

This method allows installing the latest virus definitions. To install a product upgrade of the latest version use the Automatic update.

Important
Use the manual update when the automatic update can not be performed or when the computer is not connected to the Internet.

There are 2 ways to perform the manual update:

- With `weekly.exe` file;
- With `zip archives`.

10.2.1. Manual update with `weekly.exe`

The update package `weekly.exe` is released every Friday and it includes all the virus definitions and scan engines updates available up to the release date.

To update BitDefender using `weekly.exe`, follow the next steps:

1. Download weekly.exe and save it locally on your hard disk.
2. Locate the downloaded file and double-click it to launch the update wizard.
3. Click **Next**.
4. Check **I accept the terms in the License Agreement** and click **Next**.
5. Click **Install**.
6. Click **Finish**.

10.2.2. Manual update with `zip archives`

There are two zip archives on the update server, containing the updates of the scanning engines and virus signatures: `cumulative.zip` and `daily.zip`.

- `cumulative.zip` is released every week on Monday and it includes all the virus definitions and scan engines updates up to the release date.

- `daily.zip` is released each day and it includes all the virus definitions and scan engines updates since the last cumulative and up to the current date.

BitDefender uses a service-based architecture. Because of this the procedure to replace the virus definitions is different depending on the operating system:

- Windows NT-SP6, Windows 2000, Windows XP.
- Windows 98, Windows Millennium.

Windows NT-SP6, Windows 2000, Windows XP

Steps to be followed:

1. **Download the appropriate update.** If it is Monday, please download the cumulative.zip and save it somewhere on your disk when prompted. Otherwise please download the daily.zip and save it on your disk. If this is the first time you update using the manual updates, please download the both archives.

2. **Stop BitDefender antivirus protection.**

   - **Exit BitDefender management console.** Right-click BitDefender's icon from the System Tray and select **Exit**.
   - **Open Services.** Click **Start**, then **Control Panel**, double-click **Administrative Tools** and click **Services**.
   - **Stop BitDefender Virus Shield service.** Select **BitDefender Virus Shield** service from the list and click **Stop**.
   - **Stop BitDefender Scan Server service.** Select **BitDefender Scan Server** service from the list and click **Stop**.

3. **Extract the archive content.** Start with `cumulative.zip` when both update archives are available. Extract the content in the folder `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` and accept overwriting existing files.

4. **Restart BitDefender antivirus protection.**

   - **Start BitDefender Scan Server service.** Select **BitDefender Scan Server** service from the list and click **Start**.

- **Start BitDefender Virus Shield service.** Select **BitDefender Virus Shield** service from the list and click **Start**.
- Open BitDefender management console.

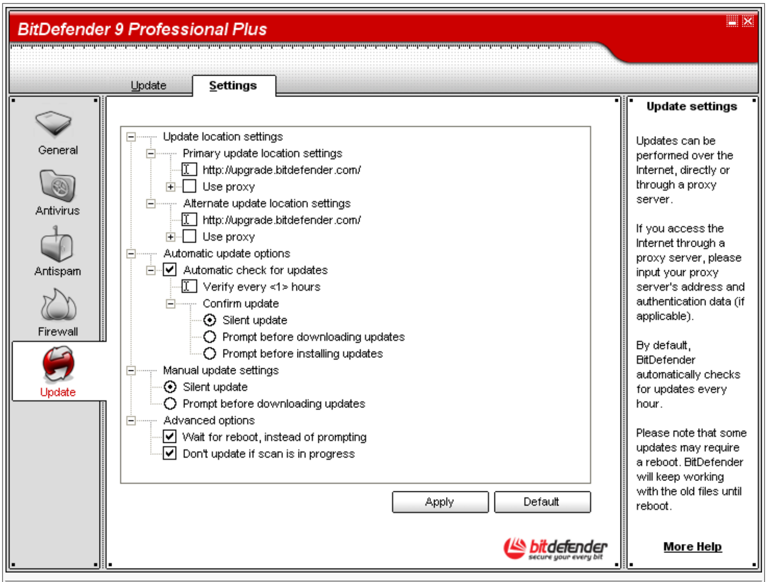
Windows 98, Windows Millennium

Steps to be followed:

1. **Download the appropriate update.** If it is Monday, please download the cumulative.zip and save it somewhere on your disk when prompted. Otherwise please download the daily.zip and save it on your disk. If this is the first time you update using the manual updates, please download the both archives.
2. **Extract the archive content.** Start with `cumulative.zip` when both update archives are available. Extract the content in the folder `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` and accept overwriting existing files.
3. **Restart the computer.**

10.3. Update settings

To access this section click **Update** tab from the **Settings** module.



- ⊟ Update location settings
  - ⊟ Primary update location settings
    - http://upgrade.bitdefender.com/
    - ⊞ □ Use proxy
  - ⊟ Alternate update location settings
    - http://upgrade.bitdefender.com/
    - ⊞ □ Use proxy
- ⊟ Automatic update options
  - ⊟ ☑ Automatic check for updates
    - Verify every <1> hours
    - ⊟ Confirm update
      - ● Silent update
      - ○ Prompt before downloading updates
      - ○ Prompt before installing updates
- ⊟ Manual update settings
  - ● Silent update
  - ○ Prompt before downloading updates
- ⊟ Advanced options
  - ☑ Wait for reboot, instead of prompting
  - ☑ Don't update if scan is in progress

Update settings

Updates can be performed over the Internet, directly or through a proxy server.

If you access the Internet through a proxy server, please input your proxy server's address and authentication data (if applicable).

By default, BitDefender automatically checks for updates every hour.

Please note that some updates may require a reboot. BitDefender will keep working with the old files until reboot.

Update Settings

The updates can be performed from the local network, over the Internet, directly or through a proxy server.

The window with the update settings contains 4 categories of options (**Update location settings**, **Automatic update options**, **Manual update settings** and **Advanced options**) organized in an expandable menu, similar to the ones from Windows.

Note

Click the box labeled "+" to open a category or click the one labeled "-" to close it.

10.3.1. Update location settings

For more reliable and faster updates, you can configure two update locations: a **Primary update location** and an **Alternate update location**. For both of them you must configure the following options:

- **Update location** - If you are connected to a local network that has BitDefender virus signatures placed locally, you can change the location of the updates here. By default this is: http://upgrade.bitdefender.com.
- **Use proxy** - In case the company uses a proxy server check this option. The following settings must be specified:
  - **Proxy sets** - type in the IP or the name of the proxy server and the port BitDefender uses to connect to the proxy server.

    Important
    Syntax: `name:port` or `ip:port`.

  - **Proxy user** - type in a user name recognized by the proxy.

    Important
    Syntax: `domain\user`.

  - **Proxy password** - type in the valid password for the previously specified user.

10.3.2. Automatic update options

- **Automatic check for updates** - BitDefender automatically checks our servers for available updates.
- **Verify every x hours** - Sets how often BitDefender checks for updates. The default time interval is 1hour.
- **Silent update** - BitDefender automatically downloads and implements the update.
- **Ask before download** - every time an update is available, you will asked before download.
- **Ask before install** - every time an update was downloaded, you will asked before installing it.

Important
If you select **Ask before download** or **Ask before install** and you close&exit the management console the automatic update will not be performed.

10.3.3. Manual update settings

- **Silent update** - the manual update will be made automatically in background.
- **Ask before download** - every time you perform a manual update you will asked before downloading and installing the updates.

Important
If you select **Ask before download** and you close&exit the management console the manual update will not be performed.

10.3.4. Advanced options

- **Wait for reboot, instead of prompting** - If an update requires a reboot, the product will keep working with the old files until the system is rebooting. The user will not be prompted for rebooting, therefore the BitDefender update process will not interfere with the user's work.
- **Don't update if scan is in progress** - BitDefender will not update if a scan process is running. This way, the BitDefender update process will not interfere with the scan tasks.

Note
If BitDefender is updated while a scan is in progress, the scan process will be aborted.

Click **Apply** to save the changes or click **Default** to load the default settings.

Best practices

11. Best practices

The **Best practices** section of this user guide contains the following topics:

- Antivirus
- Antispam

11.1. Antivirus

Steps to be followed in order to ensure a virus&spyware-free computer:

1. After the installation process is over, please register your product, as described in the "*Product registration*" (p. 49) section
2. Perform an update by user request of your virus&spyware signatures as described in the "*Automatic update*" (p. 129) section.
3. Perform a full scan of your system as described in the " *Immediate scanning* " (p. 65) section.
4. In the Status section of the **General** module, keep enabled the most important antivirus features of BitDefender: **Virus Shield**, **Firewall** and **Automatic update**.
5. Program your BitDefender to scan your system at least once a week as described in the "*Scheduled scanning*" (p. 74) section.

11.2. Antispam

Steps to be followed in order to keep Spam away from your computer:

1. If you are using Microsoft Outlook or Microsoft Outlook Express, follow the configuration wizard that opens the first time you access your e-mail client. You can also open it from the "*Antispam toolbar*" (p. 98).
2. Add the addresses of the people you absolutely need to receive mail from to the Friends list.

Note
BitDefender does not block messages from those on the list; therefore, adding friends helps ensure that legitimate messages get through.

3. Train the “ *Bayesian filter* ” (p. 38). Every time you receive an e-mail that you consider as spam, but BitDefender didn’t tag it please select it and from the BitDefender toolbar click the ☒ **Is Spam** button. Future messages that fit the same patterns will be tagged as SPAM.

Note
The **Bayesian filter** activates only after you trained it with more than 60 legitimate e-mail messages. For this you have to follow the configuration wizard.

4. Keep your BitDefender up-to-date.

Note
Every time you perform an update:
- new image signatures will be added to the **Image filter**;
- new links will be added to the **URL filter**;
- new rules will be added to the **Heuristic filter**.

This will help increase the effectiveness of your Antispam engine.

5. Configure the Charset filter. Most of the spam messages are written in Cyrillic and / or Asian charsets. Configure this filter if you want to reject all the e-mail messages written in these charsets.

Note
You can enable/disable each one of this filters in the Settings section from the **Antispam** module.

BitDefender Rescue CD

BitDefender 9 Professional Plus comes with a bootable CD (BitDefender Rescue CD based on LinuxDefender) capable to scan and disinfect all existing hard drives before your operating system starts.

You should use BitDefender Rescue CD any time your operating system is not working properly because of virus infections. That usually happens when you don't use an antivirus product.

The update of the virus signatures is made automatically, without user intervention each time you start the BitDefender Rescue CD.

12. Overview

LinuxDefender is a BitDefender re-mastered Knoppix distribution, which integrates the latest BitDefender for Linux security solution into the GNU/Linux Knoppix Live CD, offering instant SMTP antivirus/antispam protection and a desktop antivirus which is capable to scan and disinfect existing hard drives (including Windows NTFS partitions), remote Samba/Windows shares or NFS mount points. A web-based configuration interface to BitDefender solutions is also included.

Hot Features

- Instant email protection (Antivirus & Antispam)
- AntiVirus solutions for your hard-drive
- NTFS write support (using Captive project)
- Disinfection of infected files from Windows XP partitions

12.1. What is KNOPPIX?

Quote from http://knopper.net/knoppix:

“ KNOPPIX is a bootable CD with a collection of GNU/Linux (http://www.linux.com/) software, automatic hardware detection, and support for many graphic cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk. ”

12.2. System requirements

Before booting LinuxDefender, you must first verify if your system meets the following requirements.

Processor type
x86 compatible, minimum 166 MHz, but do not expect a great performance in this case. An i686 generation processor, at 800MHz, would make a better choice.

Memory
The minimum accepted value is 64MB, recommended is 128MB, for a better performance.

CD-ROM LinuxDefender runs from a CD-ROM, therefore a CD-ROM and a BIOS capable to boot from it is required.

Internet connection Although LinuxDefender will run with no Internet connection, the update procedures will require an active HTTP link, even through some proxy server. Therefore, for an up to date protection, the Internet connection is a MUST.

Graphical resolution A graphical resolution of 800x600 at least is recommended for the web-based administration.

12.3. Included software

BitDefender Rescue CD includes the following software packages.

- BitDefender SMTP Proxy (Antispam & Antivirus)
- BitDefender Remote Admin (web-based configuration)
- BitDefender Linux Edition (antivirus scanner) + GTK Interface
- BitDefender Documentation (PDF & HTML format)
- BitDefender Extras (Artwork, Leaflets)
- Linux-Kernel 2.6
- Captive NTFS write project
- LUFS - Linux Userland File System
- Tools for data recovery and system repairs, even for other operating systems
- Network and security analysis tools for network administrators
- Amanda backup solution
- thttpd
- Ethereal network traffic analyzer, IPTraf IP LAN Monitor
- Nessus network security auditor
- Parted, QTParted and partimage, partition resize, save & recovery solution
- Adobe Acrobat Reader
- Mozilla Firefox Web browser

12.4. BitDefender Linux Security solutions

LinuxDefender CD includes BitDefender SMTP Proxy Antivirus/Antispam for Linux, BitDefender Remote Admin (a web-based interface for configuring BitDefender SMTP Proxy) and BitDefender Linux Edition on-demand antivirus scanner.

12.4.1. BitDefender SMTP Proxy

BitDefender for Linux Mail Servers - SMTP Proxy is a secure content inspection solution, which provides antivirus and antispam protection at the gateway level, by scanning all e-mail traffic for known and unknown malware. As a result of a unique proprietary technology, BitDefender for Mail Servers is compatible with the majority of existing e-mail platforms and "RedHat Ready" certified.

This Antivirus and Antispam solution scans, disinfects and filters email traffic for any existing mail server, regardless of platform and operating system. BitDefender SMTP Proxy is started at boot time and scans all incoming email traffic. To configure BitDefender SMTP Proxy, use BitDefender Remote Admin, using the instructions below.

12.4.2. BitDefender Remote Admin

You can configure and manage BitDefender services remotely (after you have configured your network) or locally, by following the next steps:

1. Start Firefox browser and load BitDefender Remote Admin URL: https://localhost:8139 (or double-click the BitDefender Remote Admin icon from your desktop)
2. Log in with "bd" user and "bd" password
3. Choose "SMTP Proxy" on the left-hand menu
4. Set the Real SMTP server and the listening port
5. Add email domains to relay
6. Add network domains to relay
7. Choose "AntiSpam" on the left menu to configure antispam capabilities
8. Choose "AntiVirus" to configure BitDefender Antivirus actions (what to do when a virus is found, quarantine location)
9. Additionally, you can configure "Mail notifications" and logging capabilities ("Logger")

12.4.3. BitDefender Linux Edition

The antivirus scanner included in LinuxDefender is integrated directly into the desktop. This version features a GTK+ graphical interface.

Just browse your hard drive (or mounted remote shares), right click on any file or folder and select "Scan with BitDefender". BitDefender Linux Edition will scan selected items and display a status report. For fine grained options see BitDefender Linux Edition documentation (in the BitDefender Documentation folder or manual page) and the **/opt/BitDefender/lib/bdc** program.

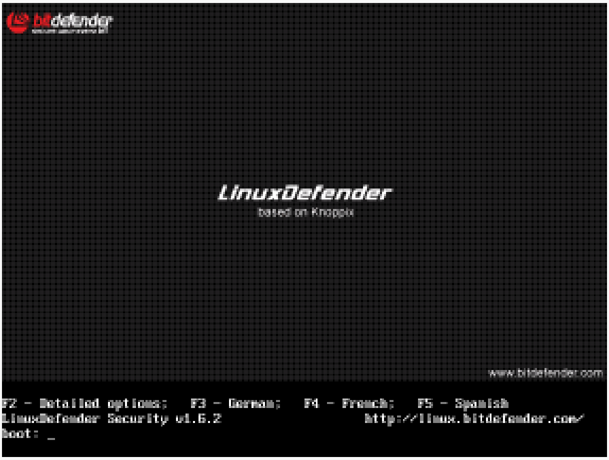
13. LinuxDefender howto

13.1. Start and stop

13.1.1. Start LinuxDefender

To start the CD, set up the BIOS of your computer to boot off the CD, put the CD in the drive and reboot the computer. Make sure that your computer can boot from CD.

Wait until the next screen shows up and follow the on-screen instructions to start LinuxDefender.

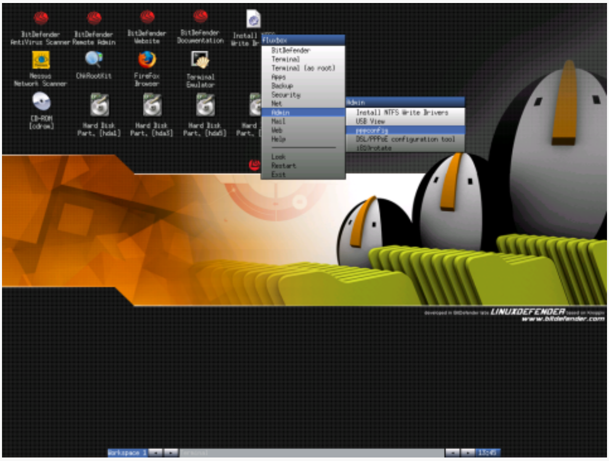


```
F2 - Detailed options;   F3 - German;   F4 - French;   F5 - Spanish
LinuxDefender Security v1.6.2                  http://linux.bitdefender.com/
boot: _
```

Boot splash screen

Press F2 for detailed options. Press F3 for detailed options in German. Press F4 for detailed options in French. Press F5 for detailed options in Spanish. For a quick start-up with default options, just press ENTER.

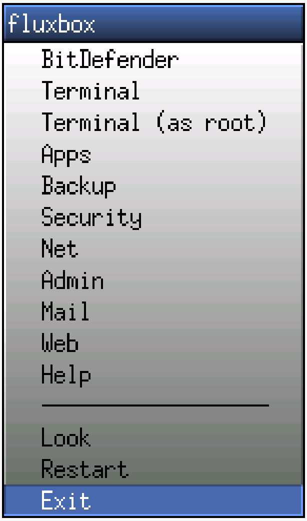
When the boot process has finished you will see the next desktop. You may now start using LinuxDefender.



The Desktop

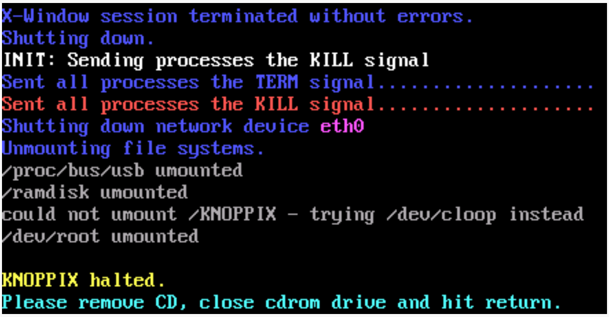
13.1.2. Stop LinuxDefender

To properly exit from LinuxDefender it's recommended to unmount all mounted partitions using **umount** command or by right-clicking the partition icons on the desktop and select **Unmount**. Then you can safely shut down your computer by selecting **Exit** from the LinuxDefender menu (right-click to open it) or by issuing the **halt** command in a terminal.



Choose "EXIT"

When LinuxDefender has succesfully closed all programs it will show a screen like the following image. You may remove the CD in order to boot from your hard drive. Now it's ok to turn off your computer or to reboot it.



```
X-Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Sent all processes the TERM signal...................
Sent all processes the KILL signal...................
Shutting down network device eth0
Unmounting file systems.
/proc/bus/usb umounted
/ramdisk umounted
could not umount /KNOPPIX - trying /dev/cloop instead
/dev/root umounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return.
```

Wait for this message when shutting down

13.2. Configure the Internet connection

If you're in a DHCP network and you have an ethernet network card, the Internet connection should already be detected and configured. For a manual configuration, follow the next steps.

1. Open the LinuxDefender menu (right-click) and select **Terminal** to open a console.
2. Type **netcardconfig** in the open terminal to launch the network configuration tool.
3. If your network is using DHCP, select **yes** (if you're not sure, ask your network administrator). Otherwise, see below.
4. The network connection should be automatically configured now. You can see your IP and network card settings with **ifconfig** command.
5. If you have a static IP (you're not using DHCP), choose **No** at the DHCP question.
6. Follow the on-screen instructions. If you're not sure what to write, contact your system or network administrator for details.

If everything goes well, you can test your Internet connection by "ping-ing" `bitdefender.com`.

```
$ ping  -c  3  bitdefender.com
```

If you're using a dial-up connection, choose **pppconfig** from the LinuxDefender / Admin menu. Then follow the on-screen instruction to set up a PPP Internet connection.

13.3. BitDefender update

The BitDefender packages for LinuxDefender are using the system's ramdisk for updatable files. This way, you can update all virus signatures, scanning engines or antispam databases, even if you're running the system from a read-only media, as the LinuxDefender CD.

Make sure that you have a working Internet connection. First open BitDefender Remote Admin and select **Live! Update** from the left menu. Press **Update Now** to check for new updates.

Alternately, you can issue the next command in a terminal.

```
# /opt/BitDefender/bin/bd  update
```

All update processes are logged into default BitDefender log. You can watch it with the next command.

```
# tail  -f /ramdisk/BitDefender/var/log/bd.log
```

If you're using a proxy for outbound connections, configure the Proxy settings in the **Live! Update** menu, **Configuration** tab.

13.4. Virus scanning

13.4.1. How do I access my Windows data?

NTFS Write Support

NTFS write support is available using the Captive NTFS write project. You need two driver files from your Windows installation: `ntoskrnl.exe` and `ntfs.sys`. Currently, only Windows XP drivers are supported. Note that you can use them to access Windows 2000/NT/2003 partitions too.

Installing NTFS drivers

To access your NTFS Windows partitions and to be able to write data on them, you have to install the NTFS drivers first. If you're not using NTFS for your Windows partitions, but FAT, or you need read-only access to your data, you can directly mount the drives and access Windows drives as any Linux drive.

To add support for NTFS partitions, you have to install the NTFS drivers first, from your hard drives, remote shares, USB sticks or from Windows Update. It's recommended to use the drivers from a known-safe location because the local drivers from the Windows host may be virused or corrupted.

Double-click **Install NTFS Write Drivers** desktop icon to run the **BitDefender Captive NTFS Installer**. Select the first option if you want to install the drivers from the local hard drive.

If the drivers are in a common location, use **Quick search** to find the drivers.

Alternately, you can specify where your drivers are found. Or you can download the drivers from Windows Update SP1.

The drivers are not installed on the hard-drive, but temporarily used by LinuxDefender to access the Windows NTFS partitions. If the program installs the NTFS drivers, you can double-click the NTFS partitions desktop icons and browse the content. For a powerful file manager, use Midnight Commander from the LinuxDefender menu (or type **mc** in a console).

13.4.2. How do I perform an antivirus scan?

Browse your folders, right-click a file or directory and select **Send to**. Then choose **BitDefender Scanner**.

Or you can issue the next command as root, from a terminal. The **BitDefender Antivirus Scanner** will start with the selected file or folder as default location to scan.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Then click **Start Scan**.

If you want to configure the antivirus options, select **Configure Antivirus** tab from the left panel of the program.

13.5. Build an instant mail filtering toaster

You can use LinuxDefender to create an ad-hoc mail filtering solution, without installing any software or modifying the mail server. The idea behind this is to put a LinuxDefender system in front of your mail server, allowing BitDefender to scan for spam and viruses all SMTP traffic and to relay it to the real mail server.

13.5.1. Prerequisites

You'll need a PC with Pentium 3 compatible CPU or newer, at least 256MB of RAM and a CD/DVD drive to boot from. The LinuxDefender system will have to receive the SMTP traffic instead of the real mail server. There are several ways to make this setup.

1. Change the IP of your real mail server and assign the old IP to the LinuxDefender system
2. Change your DNS records so that the MX entry for your domains is pointing to the LinuxDefender system
3. Setup your email clients to use the new LinuxDefender system as SMTP server
4. Change your firewall settings to forward / redirect all SMTP connections to the LinuxDefender system instead of the real mail server

LinuxDefender howto will not explain any of the above issues. For more information you may consult Linux Networking guides and Netfilter documentation.

13.5.2. The email toaster

Boot your LinuxDefender CD and wait until the X Windows system is loaded and functional.

To configure BitDefender SMTP Proxy, double-click the **BitDefender Remote Admin** icon from the desktop. The following window will appear. Use `bd` username and `bd` password to log into BitDefender Remote Admin.

After a successful login, you'll be able to configure BitDefender SMTP Proxy.

Choose **SMTP Proxy** to configure the real mail server you want to protect against spam and viruses.

Select **Email domains** tab to enter all email domains you want to accept email for.

Press the **Add Email Domain** or **Add Bulk Domains** and follow the on-screen instructions to set the relay email domains.

Select **Net domains** tab to enter all networks you want to relay email for.

Press the **Add Net Domain** or **Add Bulk Net Domains** and follow the on-screen instructions to set the relay network domains.

Select **Antivirus** from the left menu, to choose what to do when a virus is found and to configure other antivirus options.

Now, all SMTP traffic is scanned and filtered by BitDefender. By default, all virused messages are cleaned or dropped and all spam messages detected by BitDefender are tagged in the Subject with the word [SPAM]. An email header (X-BitDefender-Spam: Yes/No) is added to all emails to ease the client-side filtering.

13.6. Perform a network security audit

Beside its anti-malware, data recovery and mail filtering capabilities, LinuxDefender comes with a set of tools that perform an in-depth host & network security audit. Forensics analysis of compromised systems is also possible using the security tools included into LinuxDefender. Read this small tutorial to learn how you can start a quick security audit of your hosts or networks.

13.6.1. Check for rootkits

Before start looking for security issues on networked computers, first be sure that the LinuxDefender host is not compromised. You can perform a virus scanning of installed hard-drives, as shown in **Scan for viruses** tutorial or you can scan for Unix rootkits.

First, mount all your hard-disk partition, double-clicking their desktop icons or by using **mount** command in the console. Then double click the **ChkRootKit** icon to check the CD content or launch the **chkrootkit** command in the console, using -r NEWROOT parameter to specify the new / (root) directory of the host.

```
# chkrootkit -r /dev/hda3
```

If a rootkit is found, chkrootkit will show the finding in **BOLD**, using capital letters.

13.6.2. Nessus - the Network Scanner

What is Nessus. “ Nessus is the world's most popular open-source vulnerability scanner used in over 75,000 organizations world-wide. Many of the world's largest organizations are obtaining significant cost savings by using Nessus to audit business-critical enterprise devices and applications. ”

Nessus can be used to remotely scan your network computers against various vulnerabilities. It also recommends some measures to take to mitigate security risks and to prevent security incidents.

Double-click the **Nessus Security Scanner** desktop icon or run **startnessus** from a terminal. Wait until the following window is shown. Depending on your hardware resources, it may take up to 10 minutes for Nessus to load, along its more than 5000 plugins containing vulnerability databases. Use knoppix user and knoppix password to log in.

Click the **Target selection** tab and enter the computer IP or hostnames you want to scan for vulnerabilities. Make sure you customize all scan options according to your nework or system configuration before you start the scan in order to save tons of bandwidth and resources and have a more accurate scan result. Then click **Start the scan**.

When the scan process is complete, Nessus displays the findings and the recommendations. You can save the report in several formats, including HTML with pies and charts. The saved report can be viewed in your favorite browser.

13.7. Check your system's RAM health

Usually, when your system has an unexpected behavior (it hangs or it resets itself from time to time), it may be a memory problem. You can test your RAM modules with the **memtest** program, as described below.

Start your computer and boot from LinuxDefender CD. Type **memtest** at boot-time and press Enter.

The Memtest program will start immediately and it will run several tests to check the RAM status. You can configure what tests to run and other Memtest options, by pressing `c`.

A full Memtest run may take up to 8 hours, depending on your systems RAM capacity and speed. It's recommended to let Memtest run all its tests to entirely check for RAM errors. You can quit at any time, by pressing `ESC`.

If you intend to buy new hardware (a complete system or only some components) it's recommended to use LinuxDefender and memtest to check it for errors or compatibility issues.

Getting help

14. Support

14.1. Support Department

As a valued provider, SOFTWIN strives to provide its customers with an unparalleled level of fast and accurate support. The Support Center (which you can contact at the address indicated below) continually keeps up with the latest threats. This is where all your questions are answered in due time.

With SOFTWIN, dedication to saving customers' time and money by providing the most advanced products at the fairest prices has always been a top priority. Moreover, we believe that a successful business is based on good communication and commitment to excellence in customer support.

You are welcome to ask for support at <support@bitdefender.com> any time. For a prompt response, please include in your email as many details as you can about your BitDefender, your system and describe the problem you have encountered as accurately as possible.

14.2. On-line Help

14.2.1. BitDefender Knowledge Base

The BitDefender Knowledge Base is an online repository of information about the BitDefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bugfixing activities of the BitDefender support and development teams, along with more general articles about virus prevention, the management of BitDefender solutions with detailed explanations, and many other articles.

The BitDefender Knowledge Base is open to the public and freely searchable. The extensive information it contains is yet another means of providing BitDefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from BitDefender clients eventually find their way into the BitDefender Knowledge Base, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The BitDefender Knowledge Base is available any time at http://kb.bitdefender.com.

14.3. Contact information

Efficient communication is the key to a successful business. During the past 10 years SOFTWIN has established an unquestionable reputation by constantly striving for better communication so as to exceed the expectations of our clients and partners. Should you have any questions, do not hesitate to contact us.

14.3.1. Web Addresses

Sales department: <sales@bitdefender.com>
Technical support: <support@bitdefender.com>
Documentation: <documentation@bitdefender.com>
Partner Program: <partners@bitdefender.com>
Marketing: <marketing@bitdefender.com>
Media Relations: <pr@bitdefender.com>
Job Opportunities: <jobs@bitdefender.com>
Virus Submissions: <virus_submission@bitdefender.com>
Spam Submissions: <spam_submission@bitdefender.com>
Report Abuse: <abuse@bitdefender.com>
Product web site: http://www.bitdefender.com
Product ftp archives: ftp://ftp.bitdefender.com/pub
Local distributors: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

14.3.2. Address

The BitDefender offices are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters. Their respective addresses and contacts are listed below.

Germany

Softwin GmbH
Karlsdorfer Straße 56 88069
Tettnang
Technischer Support: <support@bitdefender.de>
Vertrieb: <vertrieb@bitdefender.de>
Phone: 07542/94 44 44
Fax: 07542/94 44 99
Product web site: http://www.bitdefender.de

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2ª planta, 08006
Barcelona
Soporte técnico: <soporte@bitdefender-es.com>
Ventas: <comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

U.S.A

BitDefender LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33308
Technical support: <support@bitdefender.us>
Sales: <sales@bitdefender.us>
Phone: 954 776 62 62, 800 388 80 62
Fax: 954 776 64 62, 800 388 80 64
Product web site: http://www.bitdefender.us

Romania

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Technical support: <suport@bitdefender.ro>
Sales: <sales@bitdefender.ro>
Phone: +40 21 2330780
Fax: +40 21 2330763
Product web site: http://www.bitdefender.ro

15. Frequently Asked Questions

1. General

Q: How can I tell if BitDefender is actually working?

A: In the **General** module, access the Status section and look at the statistics.

Q: What are the system requirements?

A: You will find them in the "*System requirements*" (p. 19) section.

Q: How do I uninstall BitDefender?

A: The removing procedure is described in the "*Removing, repairing or modifying BitDefender features*" (p. 22) section.

Q: How can I register BitDefender?

A: The registration procedure is described in the "*Product registration*" (p. 49) section.

2. Antivirus

Q: How can I perform a full system scan?

A: In the **Antivirus** module, access the Scan section, check **Local drives** and click **Scan**.

Q: How often should I scan my computer?

A: We recommend you to scan your computer at least once a week.

Q: How can I automatically scan every file that I transfer to my computer?

A: BitDefender scans all files on-access. All you have to do is to keep Virus Shield enabled.

Q: How can I program BitDefender to scan my computer periodically?

A: In the **Antivirus** module, access the Scheduler section, click **New** and follow the wizard.

Q: What happens with the files from the quarantine zone?

A: You can send these files to the BitDefender Labs in order to be analyzed, but first you must specify the e-mail settings (access the Quarantine section and click **Settings**).

3. Antispam

Q: What is spam?

A: Spam is unsolicited commercial e-mail.

Q: How does BitDefender Antispam work?

A: Please see the "*Antispam module*" (p. 35) section.

Q: Where does the spam go?

A: If you are using **Microsoft Outlook** / **Microsoft Outlook Express**, the spam messages are moved to the **Spam** folder / **Deleted Items** folder.

> **Note**
> If you are using other e-mail client you should create a rule to move the e-mail messages tagged as SPAM by BitDefender to a custom quarantine folder. BitDefender appends the prefix [SPAM] to the subject of the messages considered to be spam.

Q: I have blocked an e-mail address but I continue to receive e-mail messages from that address, why?

A: If you receive spam from an address you have blocked, please make sure that the address is not in the White list, too. The **White list** has precedence over the Black list.

Q: What is the White list?

A: It is a list of all the e-mail addresses from which you always want to receive messages, regardless of their content.

Q: What is the Black list?

A: It is a list of all the e-mail addresses from which you DON'T want to receive messages, regardless of their content.

Q: What is the Charset filter?

A: It is a filter that blocks all the e-mail messages written in Cyrillic and/or Asian.

Q: What is the Image filter?

A: It is a filter that searches the messages for images and compares those found with the images from the BitDefender database. In case of a match the e-mail will be tagged as spam.

Q: What is the URL filter?

A: It is a filter that searches the messages for links and compares those found with the links from the BitDefender database. In case of a match a spam score will be added to the e-mail.

Q: What is the Heuristic filter?

A: It is a filter that performs a set of tests on all the message components, (i.e. not only the header but also the message body in either HTML or text format), looking for words, phrases, links or other characteristics of spam. The result is that it will add a spam score to the e-mail.

Q: What is the Bayesian filter?

A: It is a filter that classifies messages according to statistical information regarding the rate at which specific words appear in messages classified Spam as compared to those declared non-Spam (by you or by the heuristic filter).

4. Firewall

Q: How can I block all Internet traffic?

A: In the **Firewall** module, Status section click **Block**.

Q: What does Program Control do?

A: The **Program Control** keeps track of all the programs connecting to the Internet and is essential for blocking Trojan horses.

Q: What does Dial Control do?

A: The **Dial Control** monitors all dialers attempting to access a computer modem, immediately warning the user and prompting him to choose whether to block or allow such operations.

Q: What does Script Control do?

A: The **Script Control** monitors all websites that are trying to activate a script or other active content. You will be in charge of which websites you trust and which you don't.

Q: What does Cookie Control do?

A: The **Cookie Control** ensures your privacy when you use the Internet.

5. Update

Q: Why is it necessary to update BitDefender?

A: Every time you perform an update new virus signatures will be added to the scan engines, new image signatures will be added to the **Image filter**, new links will be added to the **URL filter** and new rules will be added to the **Heuristic filter** and new antispyware signatures will be added to the database.

Q: How can I update BitDefender?

A: By default, BitDefender will automatically update every hour. But you can also update manually or change the time interval for the automatic update in the Update module.

Glossary

ActiveX

ActiveX is a model for writing programs so that other programs and the operating system can call them. ActiveX technology is used with Microsoft Internet Explorer to make interactive Web pages that look and behave like computer programs, rather than static pages. With ActiveX, users can ask or answer questions, use push buttons, and interact in other ways with the Web page. ActiveX controls are often written using Visual Basic.

Active X is notable for a complete lack of security controls; computer security experts discourage its use over the Internet.

Adware

Adware is often combined with a host application that is provided at no charge as long as the user agrees to accept the adware. Because adware applications are usually installed after the user has agreed to a licensing agreement that states the purpose of the application, no offense is committed.

However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these applications collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

Archive

A disk, tape, or directory that contains files that have been backed up.

A file that contains one or more files in a compressed format.

Backdoor

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

Boot sector

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot sector also contains a program that loads the operating system.

Boot virus

A virus that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the virus to become active in memory. Every time you boot your system from that point on, you will have the virus active in memory.

Browser

Short for Web browser, a software application used to locate and display Web pages. The two most popular browsers are Netscape Navigator and Microsoft Internet Explorer. Both of these are graphical browsers, which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.

Command line

In a command line interface, the user types commands in the space provided directly on the screen using command language.

Cookie

Within the Internet industry, cookies are described as small files containing information about individual computers that can be analyzed and used by advertisers to track your online interests and tastes. In this realm, cookie technology is still being developed and the intention is to target ads directly to what you've said your interests are. It's a double-edge sword for many people because on one hand, it's efficient and pertinent as you only see ads about what you're interested in. On the other hand, it involves actually "tracking" and "following" where you go and what you click. Understandably so, there is a debate over privacy and many people feel offended by the notion that they are viewed as a "SKU number" (you know, the bar code on the back of packages that gets scanned at the grocery check-out line). While this viewpoint may be extreme, in some cases it is accurate.

Disk drive

It's a machine that reads data from and writes data onto a disk.

A hard disk drive reads and writes hard disks.

A floppy drive accesses floppy disks.

Disk drives can be either internal (housed within a computer) or external (housed in a separate box that connects to the computer).

Download

To copy data (usually an entire file) from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online service to one's own computer. Downloading can also refer to copying a file from a network file server to a computer on the network.

E-mail

Electronic mail. A service that sends messages on computers via local or global networks.

Events

An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

False positive

Occurs when a scanner identifies a file as infected when in fact it is not.

Filename extension

The portion of a filename, following the final point, which indicates the kind of data stored in the file.

Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

Heuristic

A rule-based method of identifying new viruses. This method of scanning does not rely on specific virus signatures. The advantage of the heuristic scan is that it is not fooled by a new variant of an existing virus. However, it might occasionally report suspicious code in normal programs, generating the so-called "false positive".

IP

Internet Protocol - A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

Java applet

A Java program which is designed to run only on a web page. To use an applet on a web page, you would specify the name of the applet and the size (length and width, in pixels) that the applet can utilize. When the web page is accessed, the browser downloads the applet from a server and runs it on the user's machine (the client). Applets differ from applications in that they are governed by a strict security protocol.

For example, even though applets run on the client, they cannot read or write data onto the client's machine. Additionally, applets are further restricted so that they can only read and write data from the same domain that they are served from.

Macro virus

A type of computer virus that is encoded as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support powerful macro languages.

These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened.

Mail client

An e-mail client is an application that enables you to send and receive e-mail.

Memory

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips, and the word storage is used for memory that exists on tapes or disks. Every computer comes with a certain amount of physical memory, usually referred to as main memory or RAM.

Non-heuristic

This method of scanning relies on specific virus signatures. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a virus, and does not generate false alarms.

Packed programs

A file in a compression format. Many operating systems and applications contain commands that enable you to pack a file so that it takes up less memory. For example, suppose you have a text file containing ten consecutive space characters. Normally, this would require ten bytes of storage.

However, a program that packs files would replace the space characters by a special space-series character followed by the number of spaces being replaced. In this case, the ten spaces would require only two bytes. This is just one packing technique - there are many more.

Path

The exact directions to a file on a computer. These directions are usually described by means of the hierarchical filing system from the top down.

The route between any two points, such as the communications channel between two computers.

Phishing

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Polymorphic virus

A virus that changes its form with each file it infects. Since they have no consistent binary pattern, such viruses are hard to identify.

Port

An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Report file

A file that lists actions that have occurred. BitDefender maintains a report file listing the path scanned, the folders, the number of archives and files scanned, how many infected and suspicious files were found.

Script

Another term for macro or batch file, a script is a list of commands that can be executed without user interaction.

Spam

Electronic junk mail or junk newsgroup postings. Generally known as any unsolicited e-mail.

Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Startup items

Any files placed in this folder will open when the computer starts. For example, a startup screen, a sound file to be played when the computer first starts, a reminder calendar, or application programs can be startup items. Normally, an alias of a file is placed in this folder rather than the file itself.

System tray

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right click an icon to view and access the details and controls.

TCP/IP

Transmission Control Protocol/Internet Protocol - A set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

Trojan

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

BitDefender has it's own update module that allows you to manually check for updates, or let it automatically update the product.

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Virus definition

The binary pattern of a virus, used by the antivirus program to detect and eliminate the virus.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.