

bitdefender **ANTIVIRUS v10**



10th anniversary

User's guide



Antivirus
Antispyware

BitDefender Antivirus v10

User's guide

BitDefender

Published 2007.03.23

Version 10.2

Copyright© 2007 SOFTWIN

Legal Notice

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of SOFTWIN. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

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, therefore SOFTWIN is not responsible for the content of any linked site. If you access a third-party website listed in this document, 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 the third-party site.

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





Table of Contents

License and Warranty	ix
Preface	xiii
1. Conventions Used in This Book	xiii
1.1. Typographical Conventions	xiii
1.2. Admonitions	xiv
2. The Book Structure	xiv
3. Request for Comments	xv
About BitDefender	1
1. Who is BitDefender?	3
1.1. Why BitDefender?	3
Product Installation	5
2. BitDefender Antivirus v10 Installation	7
2.1. System Requirements	7
2.2. Installation Steps	7
2.3. Initial Setup Wizard	10
2.3.1. Step 1/8 - BitDefender Initial Setup Wizard	11
2.3.2. Step 2/8 - Register BitDefender Antivirus v10	11
2.3.3. Step 3/8 - Create a BitDefender Account	12
2.3.4. Step 4/8 - Enter Account Details	13
2.3.5. Step 5/8 - Learn about RTVR	14
2.3.6. Step 6/8 - Select the Tasks to Be Run	14
2.3.7. Step 7/8 - Wait for the Tasks to Complete	15
2.3.8. Step 8/8 - View Summary	16
2.4. Upgrade	16
2.5. Removing, Repairing or Modifying BitDefender	17
Description and Features	19
3. BitDefender Antivirus v10	21
3.1. Antivirus	21
3.2. Antispyware	22
3.3. Other Features	22
4. BitDefender Modules	25
4.1. General Module	25
4.2. Antivirus Module	25
4.3. Antispyware Module	25
4.4. Update Module	26

Management Console	27
5. Overview	29
5.1. System Tray	30
5.2. Scan Activity Bar	31
6. General Module	33
6.1. Central Administration	33
6.1.1. Quick Tasks	34
6.1.2. Security Level	34
6.1.3. Registration Status	35
6.2. Management Console Settings	36
6.2.1. General Settings	36
6.2.2. Virus Report Settings	37
6.2.3. Skin Settings	38
6.2.4. Manage Settings	38
6.3. Events	39
6.4. Product Registration	40
6.4.1. Registration Wizard	40
6.5. About	45
7. Antivirus Module	47
7.1. On-access Scanning	47
7.1.1. Protection Level	48
7.2. On-demand Scanning	52
7.2.1. Scan Tasks	53
7.2.2. Shortcut Menu	54
7.2.3. Scan Task Properties	54
7.2.4. On-demand Scan Types	63
7.2.5. Rootkit Scanning	67
7.3. Quarantine	68
8. Antispyware Module	71
8.1. Antispyware Status	72
8.1.1. Protection Level	73
8.2. Advanced Settings - Privacy Control	73
8.2.1. Configuration Wizard	74
8.2.2. Managing the Rules	77
8.3. Advanced Settings - Registry Control	78
8.4. Advanced Settings - Dial Control	80
8.4.1. Configuration Wizard	82
8.5. Advanced Settings - Cookie Control	84
8.5.1. Configuration Wizard	85
8.6. Advanced Settings - Script Control	87
8.6.1. Configuration Wizard	88
8.7. System Information	90
9. Update Module	91



9.1. Automatic Update	91
9.2. Manual Update	92
9.2.1. Manual Update with <code>weekly.exe</code>	93
9.2.2. Manual Update with <code>zip</code> archives	93
9.3. Update Settings	95
9.3.1. Update Location Settings	95
9.3.2. Automatic Update Options	96
9.3.3. Manual Update Settings	97
9.3.4. Advanced Options	97

Best Practices 99

10. Best Practices	101
10.1. How to Protect Your Computer against Malware Threats	101
10.2. How to Configure a Scan Task	102

BitDefender Rescue CD 103

11. Overview	105
11.1. What is KNOPPIX?	105
11.2. System Requirements	105
11.3. Included Software	106
11.4. BitDefender Linux Security Solutions	106
11.4.1. BitDefender SMTP Proxy	106
11.4.2. BitDefender Remote Admin	107
11.4.3. BitDefender Linux Edition	107

12. LinuxDefender Howto	109
12.1. Start and Stop	109
12.1.1. Start LinuxDefender	109
12.1.2. Stop LinuxDefender	110
12.2. Configure the Internet Connection	111
12.3. BitDefender Update	112
12.4. Virus Scanning	112
12.4.1. How do I access my Windows data?	112
12.4.2. How do I perform an antivirus scan?	113
12.5. Build an Instant Mail Filtering Toaster	113
12.5.1. Prerequisites	114
12.5.2. The email toaster	114
12.6. Perform a Network Security Audit	115
12.6.1. Check for Rootkits	115
12.6.2. Nessus - the Network Scanner	115
12.7. Check Your System's RAM Health	116

Getting Help 117

13. Support	119
--------------------------	------------

13.1. Support Department 119

13.2. On-line Help 119

 13.2.1. BitDefender Knowledge Base 119

13.3. Contact Information 120

 13.3.1. Web Addresses 120

 13.3.2. Branch Offices 120

Glossary 123



License and Warranty

IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS DO NOT INSTALL THE SOFTWARE. BY SELECTING "I ACCEPT", "OK", "CONTINUE", "YES" OR BY INSTALLING OR USING THE SOFTWARE IN ANY WAY, YOU ARE INDICATING YOUR COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS OF THIS AGREEMENT.

These Terms cover BitDefender Solutions and Services for home-users licensed to you, including related documentation and any update and upgrade of the applications delivered to you under the purchased license or any related service agreement as defined in the documentation and any copy of these items.

This License Agreement is a legal agreement between you (either an individual or a legal person) and SOFTWIN for use of SOFTWIN's software product identified above, which includes computer software and services, and may include associated media, printed materials, and "online" or electronic documentation (hereafter designated as "BitDefender"), all of which are protected by international copyright laws and international treaties. By installing, copying or 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.

BitDefender License. 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, limited, non-transferable and royalty-bearing license to use BitDefender.

APPLICATION SOFTWARE. You may install and use BitDefender, on as many computers as necessary with the limitation imposed by the total number of licensed users. You may make one additional copy for back-up purpose.

DESKTOP USER LICENSE. This license applies to BitDefender software that can be installed on a single computer and which does not provide network services. Each primary user may install this software on a single computer and may make one additional copy for backup on a different device. The number of primary users allowed is the number of the users of the license.

TERM OF LICENSE. The license granted hereunder shall commence on the purchasing date of BitDefender and shall expire at the end of the period for which the license is purchased.

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 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 by more than the total number of licensed users. The terms and conditions of this license replace and supersede any previous agreements that may have existed between you and SOFTWIN regarding the original product or the resulting upgraded product.

COPYRIGHT. All rights, titles 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. 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, lease or share the BitDefender license. 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.

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, SOFTWIN DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE PRODUCTS, ENHANCEMENTS, MAINTENANCE OR SUPPORT RELATED THERETO, OR ANY OTHER MATERIALS (TANGIBLE OR INTANGIBLE) OR SERVICES SUPPLIED BY HIM. SOFTWIN HEREBY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES AND CONDITIONS, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON INTERFERENCE, ACCURACY OF DATA, ACCURACY OF INFORMATIONAL CONTENT, SYSTEM INTEGRATION, AND NON



INFRINGEMENT OF THIRD PARTY RIGHTS BY FILTERING, DISABLING, OR REMOVING SUCH THIRD PARTY'S SOFTWARE, SPYWARE, ADWARE, COOKIES, EMAILS, DOCUMENTS, ADVERTISEMENTS OR THE LIKE, WHETHER ARISING BY STATUTE, LAW, COURSE OF DEALING, CUSTOM AND PRACTICE, OR TRADE USAGE.

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 to 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.

GENERAL. This Agreement will be governed by the laws of Romania and by international copyright regulations and treaties. The exclusive jurisdiction and venue to adjudicate any dispute arising out of these License Terms shall be of the courts of Romania.

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. All other trademarks used in the product or in associated materials are the property of their respective owners.

The license will terminate immediately without notice if you are in breach of any of its terms and conditions. You shall not be entitled to a refund from SOFTWIN or any resellers of BitDefender as a result of termination. The terms and conditions concerning confidentiality and restrictions on use shall remain in force even after any termination.

SOFTWIN may revise these Terms at any time and the revised terms shall automatically apply to the corresponding versions of the Software distributed with the revised terms. If any part of these Terms is found void and unenforceable, it will not affect the validity of rest of the Terms, which shall remain valid and enforceable.

In case of controversy or inconsistency between translations of these Terms to other languages, the English version issued by SOFTWIN shall prevail.

Contact SOFTWIN, at 5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, or at Tel No: 40-21-2330780 or Fax:40-21-2330763, e-mail address: [<office@bitdefender.com>](mailto:office@bitdefender.com).



Preface

This guide is intended to all users who have chosen **BitDefender Antivirus v10** 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 Antivirus v10**, 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 Antivirus v10**, 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
<code>sample syntax</code>	Syntax samples are printed with <code>monospaced</code> characters.
http://www.bitdefender.com	The URL link is pointing to some external location, on http or ftp servers.
<code><support@bitdefender.com></code>	E-mail addresses 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 <code>monospaced</code> font.
option	All the product options are printed using strong characters.
<code>sample code listing</code>	The code listing is printed with <code>monospaced</code> 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 7 parts, containing the major topics: About BitDefender, 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.

About BitDefender. A short introduction to BitDefender.

Product Installation. Step by step instructions for installing BitDefender on a workstation. This is a comprehensive tutorial on installing **BitDefender Antivirus v10**. 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. **BitDefender Antivirus v10**, 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 Antivirus v10**, how to register the product, how to scan your computer, how to perform the updates. You are taught how to configure and use all BitDefender modules.

Best Practices. Follow these instructions in order to make the best of your BitDefender.

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.

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>](mailto:documentation@bitdefender.com).



Important

Please write all of your documentation-related e-mails in English so that we can process them efficiently.



About BitDefender



1. Who is BitDefender?

BitDefender is a leading global provider of security solutions that satisfy the protection requirements of today's computing environment. The company offers one of the industry's fastest and most effective lines of security software, setting new standards for threat prevention, timely detection and mitigation. BitDefender delivers products and services to over 41 million home and corporate users in more than 180 countries. BitDefender has offices in the **United States**, the **United Kingdom**, **Germany**, **Spain** and **Romania**.

- Features antivirus, firewall, antispyware, antispam and parental control for corporate and home users;
- The BitDefender range of products is intended to be implemented on complex IT structures (work stations, file servers, mail servers, and gateway), on Windows, Linux and FreeBSD platforms;
- Worldwide distribution, products available in 18 languages;
- Easy to use, with an installation wizard that guides users through the installation process and only asks a few questions;
- Internationally certified products: Virus Bulletin, ICSA Labs, Checkmark, IST Prize, etc;
- Round the clock customer care – the customer care team is available 24 hours, 7 days a week;
- Lightning fast response time to new computer attacks;
- Best detection rate;
- Hourly Internet updates of virus signatures - automatic or scheduled actions offering protection against the newest viruses.

1.1. 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.

Further information about BitDefender can be obtained by visiting: <http://www.bitdefender.com>.



Product Installation



2. BitDefender Antivirus v10 Installation

The **BitDefender Antivirus v10 Installation** section of this user guide contains the following topics:

- System Requirements
- Installation Steps
- Initial Setup Wizard
- Upgrade
- Removing, Repairing or Modifying BitDefender

2.1. System Requirements

For proper functioning of the product, before installation, make sure that one of the following operating systems runs on your computer and that the corresponding system requirements are met:

Microsoft Windows 98 SE / NT-SP6 / Me / 2000 / XP 32-bit

- Pentium II 350 MHz or higher processor
- Minimum 128 MB of RAM Memory (256 MB recommended)
- Minimum 60 MB available hard disk space
- Internet Explorer 5.5 or higher

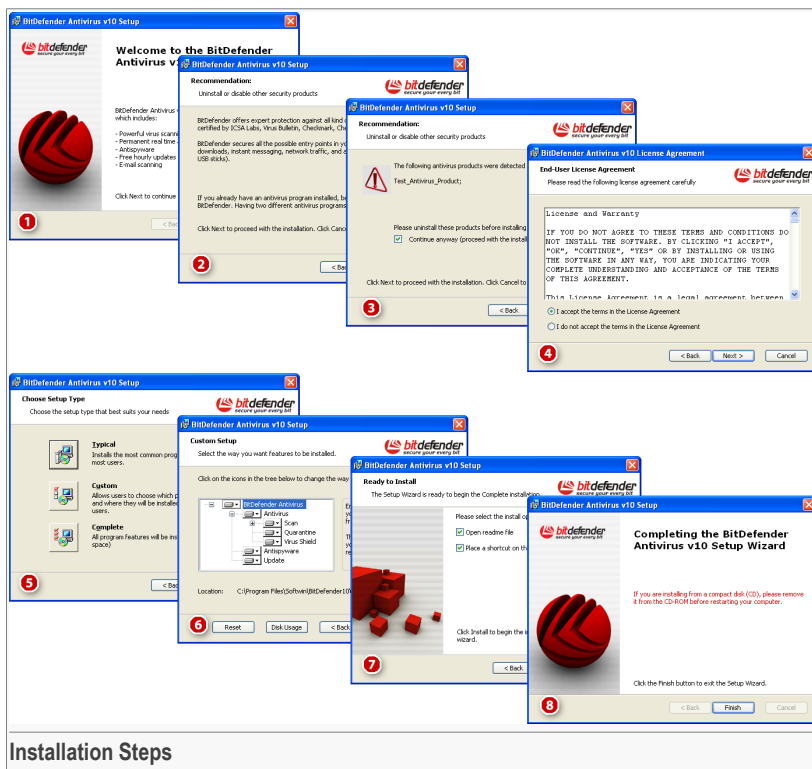
Microsoft Windows Vista 32-bit

- 800 MHz processor or higher
- Minimum 512 MB of RAM Memory (1 GB recommended)
- Minimum 60 MB available hard disk space

BitDefender Antivirus v10 can be downloaded for evaluation from <http://www.bitdefender.com> the SOFTWIN corporate website dedicated to data security.

2.2. 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

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. BitDefender Antivirus v10 alerts you if you have other antivirus products installed on your computer.



Warning

It is highly recommended that you uninstall any other antivirus products detected before installing BitDefender. Running two or more antivirus products at the same time on a computer usually renders the system unusable.

Click **Back** to return to the previous step or **Cancel** to exit setup. If you want to continue, click **Next**.

**Note**

If BitDefender Antivirus v10 does not detect other antivirus products on your system, you will skip this step.

4. 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.
5. 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 6.

6. 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 to install the selected module.

You can select the folder where you want to install the product. The default folder is `C:\Program Files\Softwin\BitDefender 10`.

If you want to select another folder, click **Browse** and in the window that opens, select the folder in which you would like BitDefender Antivirus v10 installed. Click **Next**.

7. You have two options selected by default:
 - **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 Antivirus v10 on your desktop at the end of the installation.
 - **Turn off Windows Defender** - to turn off Windows Defender; this option appears only on Windows Vista.

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



Important

During the installation process a **wizard** will appear. The wizard helps you register your **BitDefender Antivirus v10**, create a BitDefender account and set BitDefender to perform important security tasks.

Complete the wizard-guided process in order to go to the next step.

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 10`.



Note

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

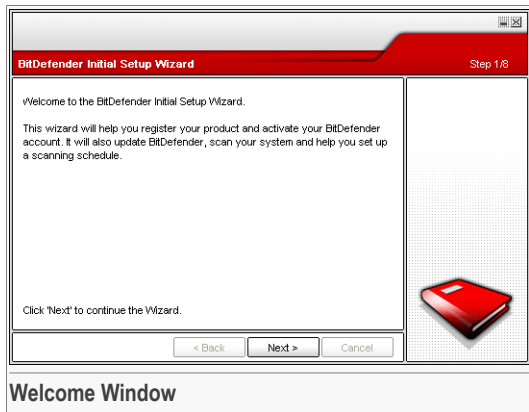
2.3. Initial Setup Wizard

During the installation process a wizard will appear. The wizard helps you register your **BitDefender Antivirus v10**, create a BitDefender account and set BitDefender to perform important security tasks.

Completing this wizard is not mandatory; however, we recommend you do so in order to save time and ensure your system is safe even before BitDefender Antivirus v10 is installed.

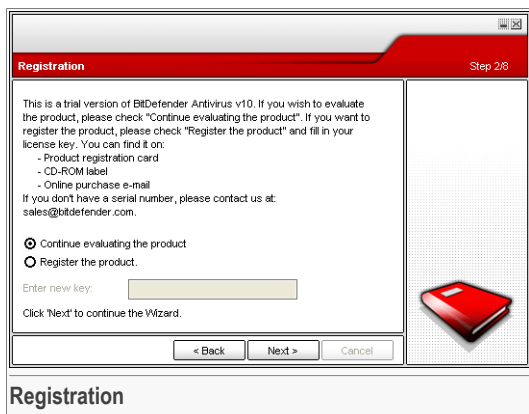


2.3.1. Step 1/8 - BitDefender Initial Setup Wizard



Click **Next**.

2.3.2. Step 2/8 - Register BitDefender Antivirus v10



Choose **Register the product** to register **BitDefender Antivirus v10**. Type the license key in the **Enter new key** field.

To continue evaluating the product, select **Continue evaluating the product**.

Click **Next**.

2.3.3. Step 3/8 - Create a BitDefender Account

Register the Product Step 3/8

You need to create an account to have access to BitDefender technical support and other personalized BitDefender services. If you already have a BitDefender account please fill in the data required. If you do not have a BitDefender account, please fill in your e-mail address and a password.

E-mail:

Password:

Retype password:

☐ Skip this step

[Forgot your password?](#)

Click 'Next' to continue or 'Cancel' to exit the Wizard.

< Back Next > Cancel

Account Creation

I do not have a BitDefender account

In order to benefit from free BitDefender technical support and other free services you need to create an account.

Type a valid e-mail address in the **E-mail** field. Think of a password and type it in the **Password** field. Confirm the password in the **Re-type password** field. Use the e-mail address and the password to log in to your account at <http://myaccount.bitdefender.com>.



Note

The password must be least four characters long.

To successfully create an account you must first activate your e-mail address. Check your e-mail address and follow the instructions in the e-mail sent to you by the BitDefender registration service.



Important

Please activate your account before moving on to the next step.

If you do not want to create a BitDefender account, just select **Skip this step**. You will also skip the next step of the wizard.

Click **Next** to continue or **Cancel** to exit the wizard.



I already have a BitDefender account

If you already have an active account, provide the e-mail address and the password of your account. If you provide an incorrect password, you will be prompted to re-type it when you click **Next**. Click **Ok** to enter the password again or **Cancel** to exit the wizard.

If you have forgotten your password, click **Forgot your password?** and follow the instructions.

Click **Next** to continue or **Cancel** to exit the wizard.

2.3.4. Step 4/8 - Enter Account Details

Configure My Account Step 4/8

Please fill in the account information. The data you provide here will be kept confidential. If you already had an account, the wizard will display the information you provided when you first created it.

First name:

Last name:

Country:

Click "Next" to continue or "Cancel" to exit the Wizard.

< Back Next > Cancel

Account Details



Note

You will not go through this step if you have selected **Skip this step** in the [third step](#).

Fill in your first and last name, and select the country in which you reside.

If you already have an account, the wizard will display the information you provided previously, if any. Here you can modify this information if you wish.

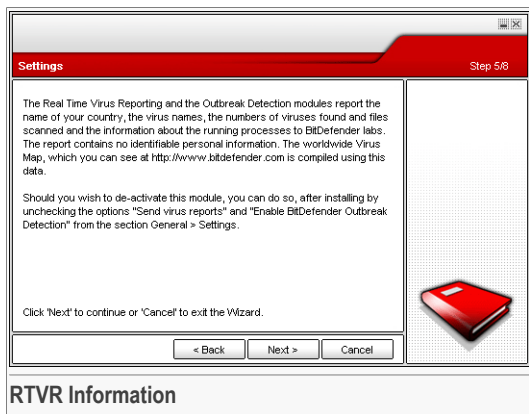


Important

The data you provide here will remain confidential.

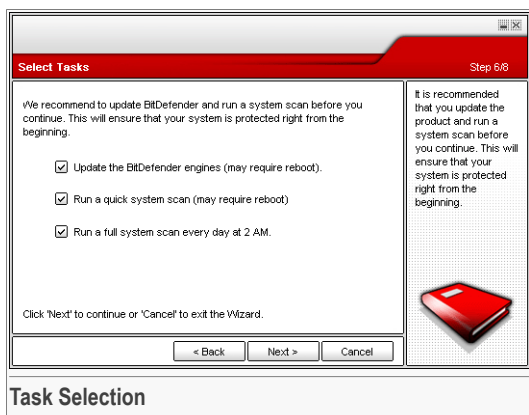
Click **Next** to continue or **Cancel** to exit the wizard.

2.3.5. Step 5/8 - Learn about RTVR



Click **Next** to continue or **Cancel** to exit the wizard.

2.3.6. Step 6/8 - Select the Tasks to Be Run



Set BitDefender Antivirus v10 to perform important tasks for the security of your system. The following options are available:



- **Update the BitDefender Antivirus v10 engines (may require reboot)** - during the next step, an update of the BitDefender Antivirus v10 engines will be performed in order to protect your computer against the latest threats.
- **Run a quick system scan (may require reboot)** - during the next step, a quick system scan will be run so as to allow BitDefender Antivirus v10 to make sure that your files from the `Windows` and `Program Files` folders are not infected.
- **Run a full system scan every day at 2 AM** - runs a full system scan every day at 2 AM.

**Important**

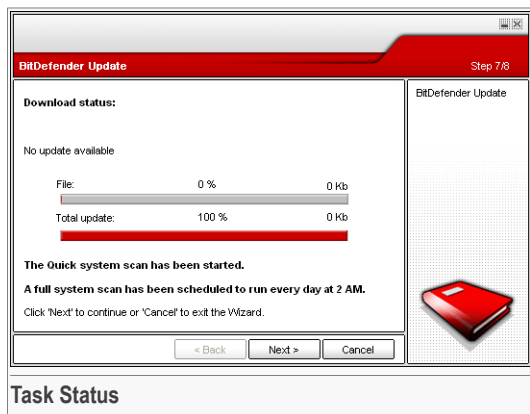
We recommend that you have these options enabled before moving on to the next step in order to ensure the security of your system.

If you select only the last option or no option at all, you will skip the next step.

You can make any changes you want by returning to the previous steps (click **Back**). Further on, the process is irreversible: if you choose to continue, you will not be able to return to the previous steps.

Click **Next** to continue or **Cancel** to exit the wizard.

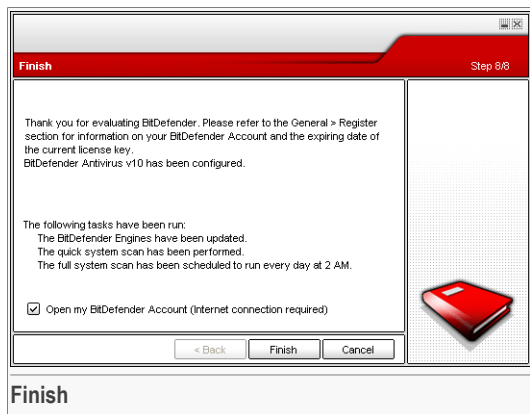
2.3.7. Step 7/8 - Wait for the Tasks to Complete



Wait for the task(s) to complete. You can see the status of the task(s) selected in the previous step.

Click **Next** to continue or **Cancel** to exit the wizard.

2.3.8. Step 8/8 - View Summary



This is the final step of the configuration wizard.

Select **Open my BitDefender Account** to enter your BitDefender account. Internet connection is required.

Click **Finish** to complete the wizard and continue with the installation process.

2.4. Upgrade

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

- **Install without removing the previous version - for v8 or higher, Internet Security excluded**

Double-click the setup file and follow the wizard described in the *"Installation Steps"* (p. 7) 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, you must remove your previous version, then restart the computer and install the new one as described in the *"Installation Steps"* (p. 7) section.

**Important**

If you upgrade from BitDefender v8 or higher, we recommend you save the [BitDefender settings](#). After the upgrade process is over, you may load them.

2.5. Removing, Repairing or Modifying BitDefender

If you want to modify, repair or remove **BitDefender Antivirus v10**, follow the path from the Windows start menu: **Start** → **Programs** → **BitDefender 10** → **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.

**Note**

To learn how to complete the installation process check the [sixth step](#) in the *"Installation Steps" (p. 7)* section.

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

**Important**

Before repairing the product we recommend you save the [BitDefender settings](#). After the repair process is over you may reload them.

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

If you choose to remove BitDefender, you will no longer be protected against viruses, spyware and hackers. If you want the Windows Firewall and Windows Defender to be enabled after uninstalling BitDefender, select the corresponding check boxes in the next step of the wizard.

We would appreciate it if you took the time to tell us the reasons why you chose to uninstall BitDefender. Select the check box corresponding to **Send FeedBack** and complete the online form to send us your suggestions.

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



3. BitDefender Antivirus v10

The antivirus and antispymware software solution for your personal computer!

BitDefender Antivirus v10 is a powerful antivirus and antispymware tool with features that best meet your security needs. Ease of use and automatic updates make **BitDefender Antivirus** an 'install and forget' product.

3.1. Antivirus

The purpose 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.

Proactive Detection. B-HAVE (Behavioral Heuristic Analyzer in Virtual Environments) 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 yet been released.

Permanent Antivirus 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.

Rootkit Detection and Removal. A new BitDefender module looks for rootkits (malicious programs designed to control victim computers, while staying hidden) and removes them on detection.

Web scanning. Web traffic is now filtered in real-time even before reaching your browser, providing a safe and enjoyable web experience.

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

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 (Outlook™, Outlook Express™ / Windows Mail™, The Bat!™, Netscape®, etc.), without any additional configuration.

3.2. Antispyware

BitDefender monitors and prevents potential spyware threats in real-time, before they can damage your system. By making use of a comprehensive database of spyware signatures, it will keep your computer spyware-free.

Real-Time Antispyware. BitDefender monitors dozens of potential “hotspots” in your system where spyware might act, and also checks any changes made to your system and software. Known spyware threats are also blocked in real-time.

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

Privacy Protection. The privacy guard monitors HTTP (web) and SMTP (mail) traffic flowing out of your computer for what might be personal information –such as credit card numbers, Social Security numbers and other user-defined strings (e.g. bits of passwords).

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

Cookie Control. The antispyware 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.

3.3. Other Features

Deployment and Use. A setup wizard starts immediately after installation, helping users select the most appropriate update settings, implementing a scanning schedule and providing a quick path to the registration and activation of the product.

User Experience. BitDefender has redesigned the user experience, placing emphasis on ease of use and clutter avoidance. As a result, many BitDefender v10 modules require significantly less user interaction, through the convenient use of automation and machine learning.

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.

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



Rescue Disk. **BitDefender Antivirus v10** is delivered on a bootable CD. This CD can be used to analyze/repair/disinfect a compromised system which cannot be started.



4. BitDefender Modules

BitDefender Antivirus v10 contains the modules: **General**, **Antivirus**, **Antispyware** and **Update**.

4.1. General Module

BitDefender comes fully configured for maximum security.

In the **General** module you can configure the security level and perform important security tasks. Also, you can register your product and you can set the overall behavior of BitDefender.

4.2. Antivirus Module

BitDefender protects you from viruses, spyware and other malware entering your system by scanning your files, e-mail messages, downloads and all other content as it enters your system.

The protection BitDefender offers is divided into two categories:

- **On-access scanning** - prevents new viruses, spyware and other malware from entering your system. This is also called real-time protection - files are scanned as the user accesses them. BitDefender will, for example, scan a word document for known threats 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, spyware or other malware in your system. This is the classic scan initiated by the user - you choose what drive, folder or file BitDefender should scan, and BitDefender scans it - on-demand.

4.3. Antispyware Module

BitDefender monitors dozens of potential "hotspots" in your system where spyware might act, and also checks any changes made to your system and software. 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.

4.4. Update Module

New malware is found and identified every day. This is why it is very important to keep BitDefender up to date with the latest malware 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 antispware 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** - BitDefender automatically contacts the update 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 threat signatures manually.




Management Console



5. Overview

BitDefender Antivirus v10 was designed with a centralized management console, which allows the configuration of the protection options for all BitDefender modules. In other words, all you need to do is open the management console in order to have access to all modules: **Antivirus**, **Antispyware** and **Update**.

To access the management console, use the Windows Start menu, by following the path **Start** → **Programs** → **BitDefender 10** → **BitDefender Antivirus v10** or quicker, double click the  **BitDefender icon** from the system tray.



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

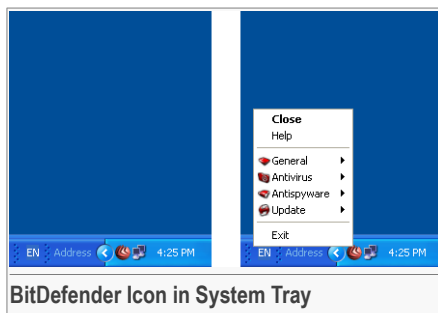
- **General** - in this section you can set the overall security level and perform essential security tasks. Here you can also register the product and see a summary of all the BitDefender main settings, product details and contact information.
- **Antivirus** - in this section you can configure the **Antivirus** module.
- **Antispyware** - in this section you can configure the **Antispyware** 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 in. The **More Help** option, placed at the bottom right, opens the **Help** file.

5.1. System Tray

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

If you double-click this icon, the management console will open. Also, by right-clicking it, a contextual menu will appear. It provides quick management of BitDefender:



- **Show / Close** - opens the management console or minimizes it to the system tray.
- **Help** - opens the help file.
- **General** - administration of the [General](#) module.
 - **Enter New Key** - starts the registration wizard that will guide you through the registration process.
 - **Edit Account** - starts a wizard that will help you create a BitDefender account.
- **Antivirus** - administration of the [Antivirus](#) module.
 - **Real-time protection is enabled / disabled** - shows the status of the [real-time protection](#) (enabled / disabled). Click this option to disable or enable the real-time protection.
 - **Scan** - opens a submenu from where you can select to run one of the scan tasks available in the [Scan](#) section.
- **Antispyware** - administration of the [Antispyware](#) module.
 - **Behavioral Antispyware is enabled / disabled** - shows the status of the [behavioral antispyware protection](#) (enabled / disabled). Click this option to disable or enable the behavioral antispyware protection.
 - **Advanced settings** - allows you to configure the antispyware controls.
- **Update** - administration of the [Update](#) module.
 - **Update Now** - performs an immediate update.
 - **Automatic update is enabled / disabled** - shows the status of the [automatic update](#) (enabled / disabled). Click this option to disable or enable the automatic 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.

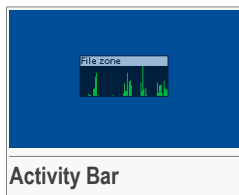
5.2. Scan Activity Bar

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

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

**Note**

The **Scan activity bar** will notify you when the Virus Shield is disabled with a red cross over the corresponding area (**File 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 the **Enable the Scan Activity bar (on screen graph of product activity)** option (from the **General** module, [Settings](#) section).



6. General Module

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

- Central Administration
- Management Console Settings
- Events
- Product Registration
- About

Note



For more details regarding the **General** module check the description of the “*General Module*” (p. 25).

6.1. Central Administration



In this section you can configure the overall security level and perform important BitDefender tasks. You can also register the product and see the expiration date.

6.1.1. Quick Tasks


BitDefender allows quick access to essential security tasks. Using these tasks you can keep your BitDefender up-to-date, scan your system or block traffic.

To scan the entire system just click  **Scan Now**. The [scan window](#) will appear and a full system scan will be initiated.



Important

We strongly recommend that you run a full system scan at least once a week. For more details about scan tasks and the scanning process check the [On-demand Scanning](#) section of this user guide.

Before scanning your system, we recommend that you update BitDefender so it can detect the latest threats. To update BitDefender just click  **Update Now**. Wait a few seconds for the update process to complete or, better, check the [Update](#) section to see the update status.



Note

For more details about the update process check the [Automatic Update](#) section of this user guide.

6.1.2. Security Level

You can choose the security level that better fits your protection needs. Drag the slider along the scale to set the appropriate security level.

There are 3 security levels:

Security level	Description
Maintenance	Offers no protection. Only the Automatic Update is enabled. Only updates BitDefender. Although it does not offer any protection this security level might be useful to system administrators.
Local System	Offers antivirus protection. Especially recommended for computers with no network or Internet access. The resource consumption level is very low. Accessed files are scanned for viruses.
Local System Plus	Offers antivirus&antispysware protection. Especially recommended for computers with no network or Internet access. The resource consumption level is low.



Security level	Description
	Accessed files are scanned for viruses and spyware.

BitDefender Antivirus v10 is recommended for computers with no network or Internet access.

You can customize the security level by clicking **Custom level**. In the window that will appear, select the BitDefender protection options you want to enable and click **OK**.

Click **Default Level** to set the slider at the default level.

6.1.3. Registration Status

You can see information about the status of your BitDefender license. Here you can register the product and see the expiration date.

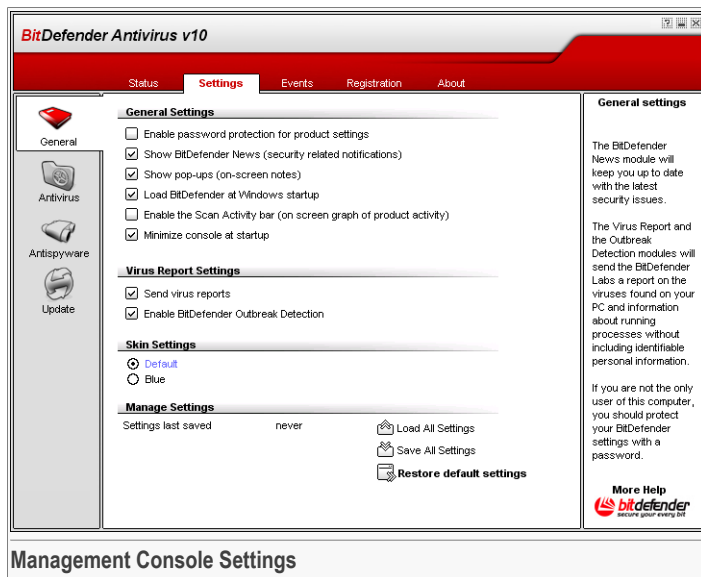
To enter a new key click  **Enter New Key**. Complete the [registration wizard](#) to successfully register BitDefender.



Note

For more details about the registration process check the [Product Registration](#) section of this user guide.

6.2. 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.

6.2.1. General Settings

- **Enable password protection for product settings** - enables setting a password in order to protect the BitDefender Management Console configuration.



Note

If you are not the only person with administrative rights 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:



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.

- **Show BitDefender News (security related notifications)** - shows from time to time security notifications regarding virus outbreaks, sent by the BitDefender server.
- **Show pop-ups (on-screen notes)** - shows pop-up windows regarding the product status.
- **Load BitDefender at Windows startup** - automatically launches BitDefender at system startup.



Note

We recommend you to keep this option selected.

- **Enable the Scan Activity bar (on screen graph of product activity)** - enables/disables the [Scan Activity Bar](#).
- **Minimize console at startup** - minimizes the BitDefender management console after it has been loaded at system startup. Only the  [BitDefender icon](#) will appear in the system tray.

6.2.2. Virus Report Settings

- **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.



- **Enable BitDefender Outbreak Detection** - sends to the BitDefender Labs reports regarding potential 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 potential virus and will be used solely to detect new viruses.

6.2.3. Skin Settings

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.

6.2.4. Manage Settings

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.



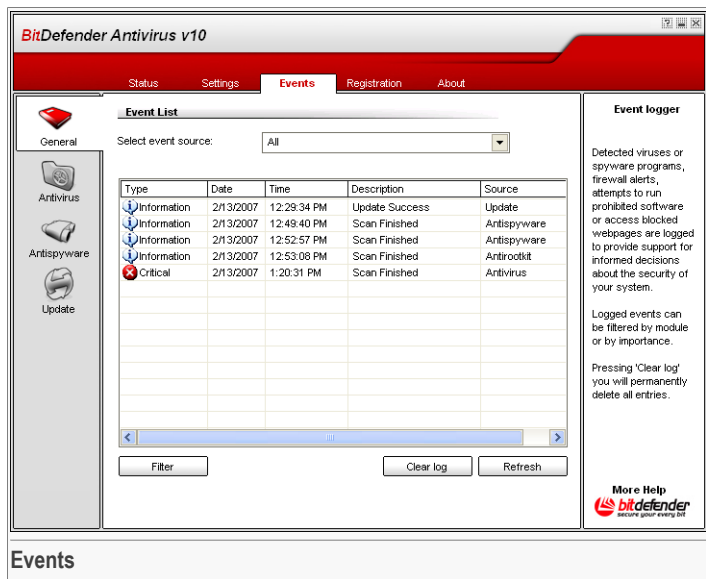
Important

Only users with administrative rights can save and load settings.

To load the default settings, click  **Restore Default Settings**.



6.3. Events



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

There are 3 types of events: **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**, **Antispyware** 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** and then **Yes** to confirm your choice.

6.4. Product Registration



This section contains information about the BitDefender product (registration status, product ID, expiration date) and the BitDefender account. Here you can register the product and configure your BitDefender account.

Click the **Buy Now** button to get a new license key from the BitDefender online store.

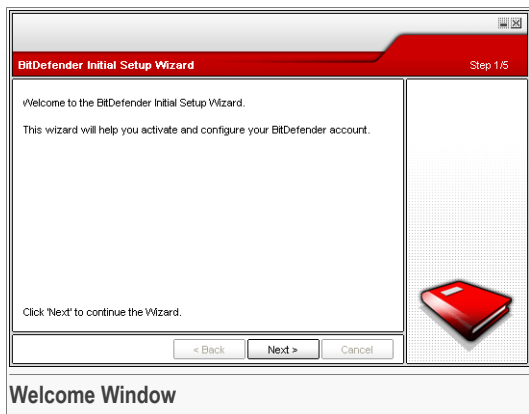
By clicking **Enter New Key** you can register the product, modify the registration key or the account details. To configure your BitDefender account click **Edit Account**. In both cases, the registration wizard will appear.

6.4.1. Registration Wizard

The registration wizard is a 5 step procedure.

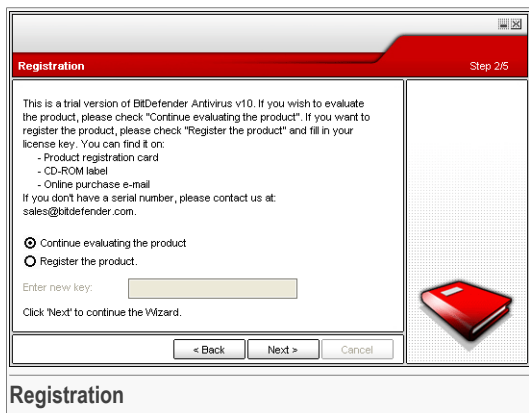


Step 1/5 - Welcome to BitDefender Registration Wizard



Click **Next**.

Step 2/5 - Register BitDefender



Choose **Register the product** to register **BitDefender Antivirus v10**. Type the license key in the **Enter new key** field.

To continue evaluating the product select **Continue evaluating the product**.

Click **Next**.

Step 3/5 - Create a BitDefender Account

Register the Product Step 3/5

You need to create an account to have access to BitDefender technical support and other personalized BitDefender services. If you already have a BitDefender account please fill in the data required. If you do not have a BitDefender account, please fill in your e-mail address and a password.

E-mail:

Password:

Retype password:

[Forgot your password?](#)

☒ Skip this step

Click 'Next' to continue or 'Cancel' to exit the Wizard.

< Back Next > Cancel

Account Creation

Please enter a valid e-mail address. A confirmation message will be sent to the address you have provided.

I do not have a BitDefender account

In order to benefit from free BitDefender technical support and other free services you need to create an account.

Type a valid e-mail address in the **E-mail** field. Think of a password and type it in the **Password** field. Confirm the password in the **Re-type password** field. Use the e-mail address and the password to log in to your account at <http://myaccount.bitdefender.com>.



Note

The password must be least four characters long.

To successfully create an account you must first activate your e-mail address. Check your e-mail address and follow the instructions in the e-mail sent to you by the BitDefender registration service.



Important

Please activate your account before moving on to the next step.

If you do not want to create a BitDefender account, just select **Skip this step**. You will also skip the next step of the wizard.

Click **Next** to continue.



I already have a BitDefender account

If you already have an active account, provide the e-mail address and the password of your account. If you provide an incorrect password, you will be prompted to re-type it when you click **Next**. Click **Ok** to enter the password again or **Cancel** to exit the wizard.

If you have forgotten your password, click **Forgot your password?** and follow the instructions.

Click **Next** to continue.

Step 4/5 - Enter Account Details

Note



You will not go through this step if you have selected **Skip this step** in the [third step](#).

Fill in your first and last name and select the country you are from.

If you already have an account, the wizard will display the information you provided previously, if any. Here you can also modify this information if you want to.

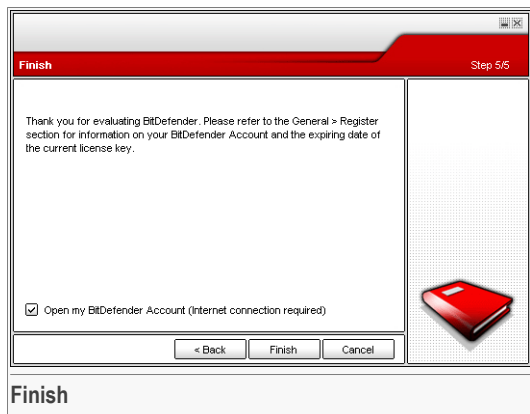


Important

The data you provide here will remain confidential.

Click **Next**.

Step 5/5 - View Summary



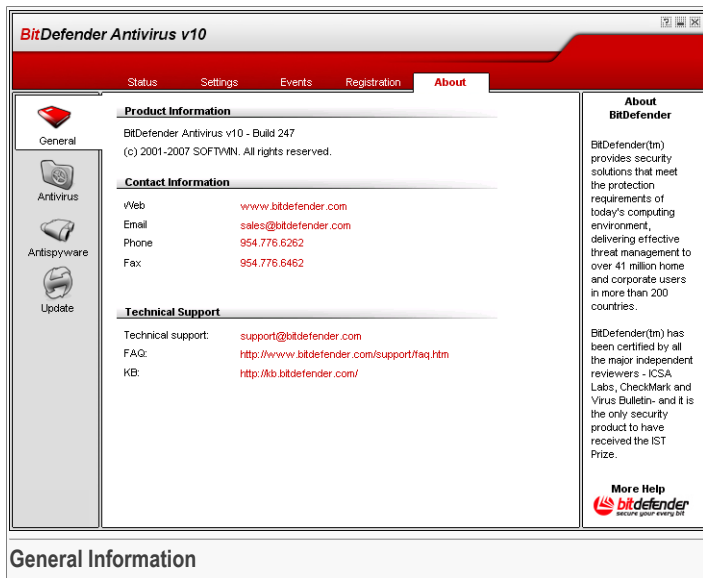
This is the final step of the configuration wizard. You can make any changes you want by returning to the previous steps (click **Back**).

If you do not want to make any changes, click **Finish** to exit the wizard.

Select **Open my BitDefender Account** to enter your BitDefender account. Internet connection is required.



6.5. About



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

BitDefender™ is a leading global provider of security solutions that satisfy the protection requirements of today's computing environment. The company offers one of the industry's fastest and most effective lines of security software, setting new standards for threat prevention, timely detection and mitigation. BitDefender delivers products and services to over 41 million home and corporate users in more than 180 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**.

Further information about BitDefender can be obtained by visiting:
<http://www.bitdefender.com>.



7. Antivirus Module

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

- On-access Scanning
- On-demand Scanning
- Quarantine



Note

For more details regarding the **Antivirus** module check the description of the “*Antivirus Module*” (p. 25).

7.1. On-access Scanning

The screenshot displays the BitDefender Antivirus v10 management console. The interface is divided into several sections:

- Shield Tab:** Contains the main settings for real-time protection.
- General:** Shows the status of real-time protection, which is currently enabled. It also indicates the last system scan was never performed.
- Protection Level:** Offers three levels: Aggressive, Default (selected), and Permissive. The Default level is described as 'Standard security, low use of resources' and lists actions like scanning all files, incoming/outgoing e-mail messages, viruses/spyware, and web traffic. It also mentions actions on infected files (Disinfect, Deny) and B-HAVE heuristic analysis.
- Statistics:** Shows the last scanned file as 'd:\bd_10\images\screenshots\av\antispysware_system.png'. It includes a 'More statistics' link and a 'Traffic' graph showing activity over time.
- Real-time protection sidebar:** Provides additional information, stating that BitDefender scans accessed files against viruses, spyware, and other malware. It also includes instructions on how to adjust the protection level using a slider.
- More Help:** A link to the BitDefender website for further assistance.

Real-time Protection

In this section you can configure the **Real-time protection** and you can view information about its activity. The **Real-time protection** keeps your computer safe by scanning e-mail messages, downloads and all accessed files.

**Important**

To prevent viruses from infecting your computer keep **Real-time protection** enabled.

In the bottom side of the section you can see the **Real-time protection** 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. Protection Level

You can choose the protection level that better fits your security needs. Drag the slider along the scale to set the appropriate protection level.

There are 3 protection levels:

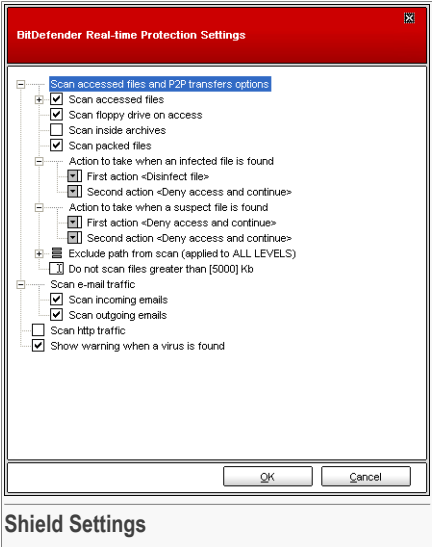
Protection level	Description
Permissive	<p>Covers basic security needs. The resource consumption level is very low.</p> <p>Programs and incoming mail messages are only scanned for viruses. Besides the classical signature-based scan, the heuristic analysis is also used. The actions taken on infected files are the following: clean file/deny access.</p>
Default	<p>Offers standard security. The resource consumption level is low.</p> <p>All files and incoming&outgoing mail messages are scanned for viruses and spyware. Besides the classical signature-based scan, the heuristic analysis is also used. The actions taken on infected files are the following: clean file/deny access.</p>
Aggressive	<p>Offers high security. The resource consumption level is moderate.</p> <p>All files, incoming&outgoing mail messages and web traffic are scanned for viruses and spyware. Besides the classical signature-based scan, the heuristic analysis is also used. The actions taken on infected files are the following: clean file/deny access.</p>

To apply the default real-time protection settings click **Default Level**.

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.



You can customize the **Real-time protection** by clicking **Custom level**. The following window will appear:



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

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.

Option		Description
Scan accessed files	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;

Option	Description
	.pdf; .msi; .ini; .csc; .cmd; .bas; .eml and .nws.
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 for riskware	Scans for riskware. These files will be treated as infected files. Software that includes adware components might stop working if this option is enabled. Select Skip dialers and applications from scan if you want to exclude these kind of files from scanning.
Scan floppy drive on access	Scans the floppy drive, when it is accessed.
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.
First action	Select from the drop-down menu the first action to take on infected and suspicious files.
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	Select from the drop-down menu the second action to take on infected files, in case the first action fails.
Deny access and continue	In case an infected file is detected, the access to this will be denied.



Option	Description
Delete file	Deletes the infected files immediately, without any warning.
Move file to quarantine	Move the infected files into the quarantine.
Do not scan files greater than [x] Kb	Type in the maximum size of the files to be scanned. If the size is 0 Kb, all files will be scanned, regardless their size.
Exclude path from scan(applied to ALL LEVELS)	<p>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, <i>New item</i>, 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.</p> <p>The objects selected here will be excluded from scanning, regardless of the protection level chosen (not only for the Custom Level).</p>

- **Scan e-mail traffic** - scans the e-mail traffic.

The following options are available:

Option	Description
Scan incoming mails	Scans all incoming e-mail messages.
Scan outgoing mails	Scans all outgoing e-mail messages.

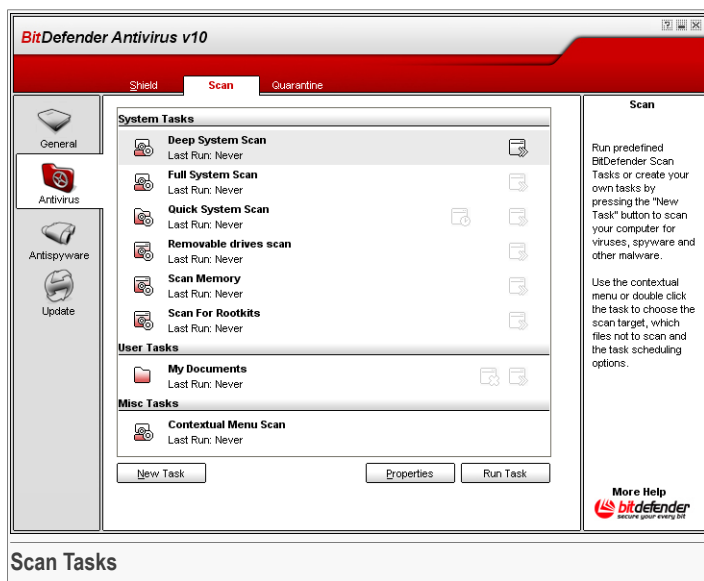
- **Scan http traffic** - scans the http traffic.
- **Show warning when a virus is found** - opens an alert window when a virus is found in a file or in an e-mail message.

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.

Click **OK** to save the changes and close the window.

7.2. On-demand Scanning



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.



7.2.1. Scan Tasks

The on-demand scan is based on scan tasks. The user can scan the computer using the default tasks or his own scan tasks (user-defined tasks).

There are three categories of scan tasks:

- **System tasks** - contains the list of default system tasks. The following tasks are available:



Default Task	Description
Deep System Scan	Scans the entire system, including archives, for viruses and spyware.
Full System Scan	Scans the entire system, except for archives, for viruses and spyware.
Quick System Scan	Scans all programs for viruses and spyware.
Removable drives scan	Scans removable drives for viruses and spyware.
Scan Memory	Scans memory for known spyware threats.
Scan for Rootkits	Scans memory for stealth malware.

- **User tasks** - contains the user-defined tasks.

A task called `My Documents` is provided. Use this task to scan your documents from the `My Documents` folder.

- **Misc tasks** - contains a list of miscellaneous scan tasks. These scan tasks refer to alternative scanning types that cannot be run from this window. You can only modify their settings or view the scan reports.

Three buttons are available to the right of each task:

-  **Schedule Task** - indicates that the selected task is scheduled for later. Click this button to go to the [Scheduler](#) section from the **Properties** windows where you can modify this setting.
-  **Delete** - removes the selected task.



Note

Not available for system tasks. You cannot remove a system task.

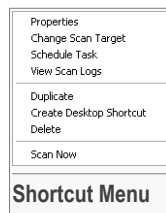
-  **Scan Now** - runs the selected task, initiating an **immediate scan**.

7.2.2. Shortcut Menu

A shortcut menu is available for each task. Right-click the selected task to open it.

The following commands are available on the shortcut menu:

- **Scan Now** - runs the selected task, initiating an immediate scan.
- **Change Scan Target** - opens the **Properties** window, **Scan Path** tab, where you can change the scan target for the selected task.
- **Schedule Task** - opens the **Properties** window, **Scheduler** tab, where you can schedule the selected task.
- **View Scan Logs** - opens the **Properties** window, **Scan Logs** tab, where you can see the reports generated after the selected task was run.
- **Duplicate** - duplicates the selected task.



Note

This is useful when creating new tasks, as you can modify the settings of the task duplicate.

- **Create Desktop Shortcut** - creates a desktop shortcut to the selected task.
- **Delete** - deletes the selected task.



Note

Not available for system tasks. You cannot remove a system task.

- **Properties** - opens the **Properties** window, **Overview** tab, where you can change the settings of the selected task.



Important

Due to their particular nature, only the **Properties** and **View Scan Logs** options are available for the tasks in the **Misc Tasks** category.

7.2.3. Scan Task Properties

Each scan task has its own **Properties** window, where you can configure the scan options, set the scan target, schedule the task or see the reports. To enter this window select the task and click **Properties** (or right-click the task and then click **Properties**).



Scan Settings

Here you can see information about the task (name, last run and schedule status) and set the scan settings.

Scan Level

First of all, you have to choose the scan level. Drag the slider along the scale to set the appropriate scan level.

Full System Scan Properties

Overview

Scan Path

Scheduler

Scan Logs

Task Properties

Task name: Full System Scan
Last Run: 2/13/2007 12:49:40 PM
Scheduled: not scheduled

Scan Level

High

Medium

Low

MEDIUM

- Standard, moderate resource consumption
- Scan all files
- Scan for viruses and spyware
- First/Second action: Disinfect files / Move to Quarantine

Custom

Default

☐ Run the task with low priority
☐ Shut down computer on scan completion
☐ Minimize scan window to Sys Tray
☐ Close scan window if no infected files are found

Scan

OK

Cancel

Scan Settings

There are 3 scan levels:

Protection level	Description
Low	<p>Offers reasonable detection efficiency. The resource consumption level is low.</p> <p>Programs only are scanned for viruses. Besides the classical signature-based scan, the heuristic analysis is also used. The actions taken on infected files are the following: clean file/move to quarantine.</p>
Medium	<p>Offers good detection efficiency. The resource consumption level is moderate.</p> <p>All files are scanned for viruses and spyware. Besides the classical signature-based scan, the heuristic analysis is also used. The actions taken on infected files are the following: clean file/move to quarantine.</p>
High	<p>Offers high detection efficiency. The resource consumption level is high.</p>

55

Protection level	Description
	All files and archives are scanned for viruses and spyware. Besides the classical signature-based scan, the heuristic analysis is also used. The actions taken on infected files are the following: clean file/move to quarantine.



Important

The **Scan for Rootkits** task has the same scan levels. However, the options are different:

- **Low** - Only processes are scanned. No action is taken on the detected objects.
- **Medium** - Files and processes are scanned in search for hidden objects. No action is taken on the detected objects.
- **High** - Files and processes are scanned in search for hidden objects. Detected objects are renamed.

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 **Custom** to set your own scan options. A new window will appear.

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:

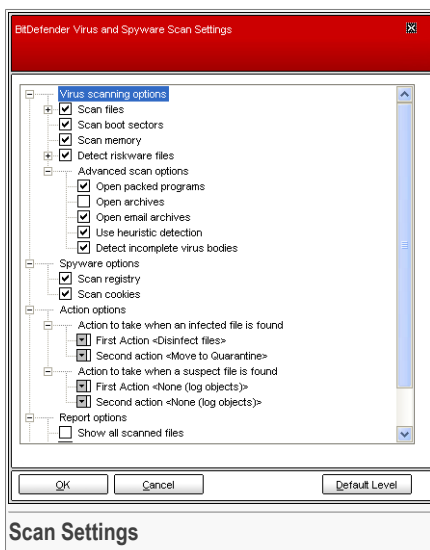
- **Virus scanning options**
- **Spyware options**
- **Action options**
- **Report options**
- **Other options**

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



Important

For the **Scan for Rootkits** task only three categories are available: **Rootkit scanning options**, **Report options** and **Other options**. From the first





category you can choose what to scan (files or memory, or both) and you can set the action taken on the detected objects (**None (log objects)/Rename files**). The last two categories are identical to the ones described below.

- 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 scanning options** category.

Option		Description
Scan files	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.
	Scan user defined extensions	Only the files with the extensions specified by the user will be scanned. 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.
Scan memory		Scans the memory for viruses and other malware.
Detect riskware files		<p>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.</p> <p>Select Except applications and dialers if you want to exclude these kind of files from scanning.</p>

Option	Description
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 (registry, cookies). This is made through the selection of certain options from **Spyware scan options** category.

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

- 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



Action	Description
	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.
Move files to Quarantine	Moves the infected files into the quarantine.
Rename files	Changes the extension of the infected files. The new extension of the infected files will be <code>.vir</code> . 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.



Important

Rename files has a similar effect on the hidden files (rootkits). The new extension of the detected files will be `.bd.ren`. By renaming the detected files, the possibility of executing and thus of spreading the potential infection is removed. At the same time they can be saved for further examination and analysis.

- 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.
Delete logs older than [x] days	This is an edit field that allows specifying how long a report should be kept in the Scan Logs section. Select this option and type in a new time interval. The default time interval is 180 days.



Note

The report files can be seen in the [Scan Logs](#) section from the **Properties** window.

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

Option	Description
Submit suspect files to BitDefender Lab	You will be prompted to submit all suspect files to BitDefender lab after the scan process has finished.

If you click **Default Level** you will load the default settings.

Click **OK** to save the changes and close the window.

Other Settings

A series of general options for the scanning process are also available:

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.

Click **OK** to save the changes and close the window. To run the task, just click **Scan**.

Scan Target

Select the task, click **Properties** and then click the **Scan Path** tab to enter this section.



Here you can set the scan target.

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

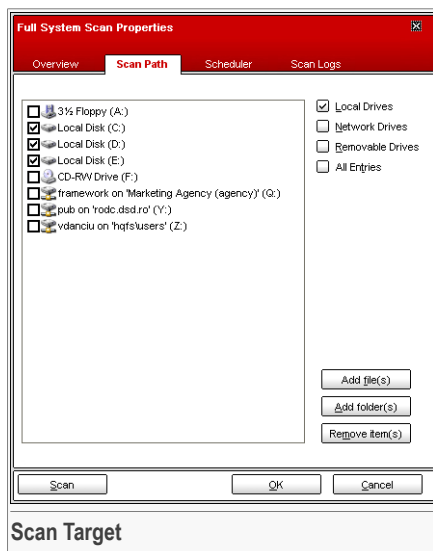
You can also use drag and drop to add files/folders to the list.

- **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.



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**.

Click **OK** to save the changes and close the window. To run the task, just click **Scan**.

Scheduler

Select the task, click **Properties** and then click the **Scheduler** tab to enter this section.

Here you can see if the task is scheduled or not and you can modify this property.



Important

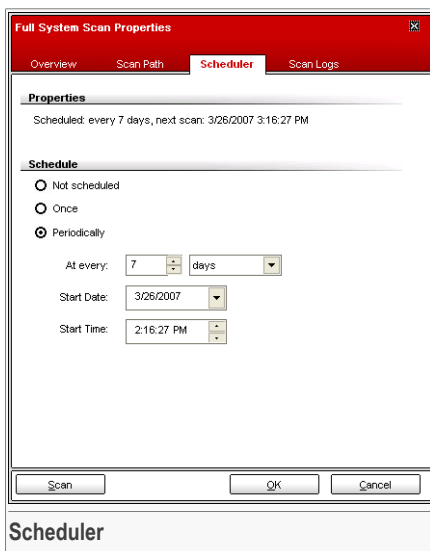
With complex tasks, the scanning process will take some time and it will work best if you close all other programs. That's why it is best for you to schedule such tasks when you are not using your computer and it has gone into the idle mode.

When scheduling a task, you must to choose one of the following options:

- **Not scheduled** - launches the task only when the user requests it.
- **Once** - launches the scan only once, at a certain moment. Specify the start date and time in the **Start Date/Time** fields.
- **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 at certain intervals, select **Periodically** and type in the **At every** edit box the number of minutes/hours/days/weeks/ months/years indicating the frequency of this process. You must also specify the start date and time in the **Start Date/Time** fields.

Click **OK** to save the changes and close the window. To run the task, just click **Scan**.



Scan Logs

Select the task, click **Properties** and then click the **Scan Logs** tab to enter this section.



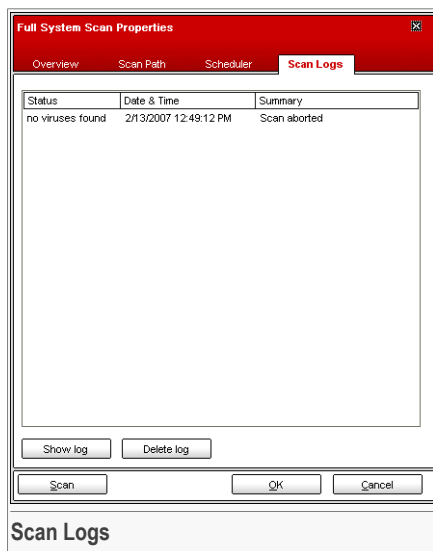
Here you can see the report files generated each time the task was executed. Each file has enclosed information on its status (clean/infected), the date and time when the scan was performed and a summary (scan finished).

Two buttons are available:

- **Show log** - to view the selected report file;
- **Delete log** - to delete the selected report file.

Also, to view or delete a file, right-click the file and select the corresponding option from the shortcut menu.

Click **OK** to save the changes and close the window. To run the task, just click **Scan**.



7.2.4. On-demand Scan Types

BitDefender allows three types of on-demand scan:

- **Immediate scanning** - run a scan task from the system / user tasks;
- **Contextual scanning** - right-click on a file or a folder and select BitDefender Antivirus v10;
- **Drag& Drop scanning** - drag and drop a file or a folder over the **Scan Activity Bar**;

Immediate Scanning


To scan your computer or part of it you can use the default scan tasks or you can create your own scan tasks. There are two methods of creating scan tasks:

- **Duplicate** an existing task, rename it and make the necessary changes in the **Properties** window;
- Click **New Task** to create a new task and **configure** it.

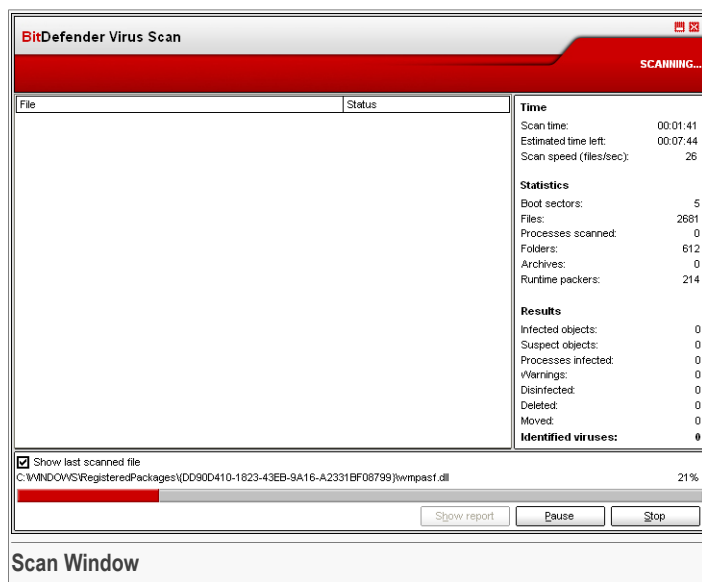
In order for BitDefender to make a complete scanning, you need to shut down all open programs. Especially your email-client (i.e. Outlook, Outlook Express or Eudora) is important to shut down.

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.

To start scanning, use one of these methods:

- double-click the desired scan task from the list.
- click the  **Scan now** button corresponding to the task.
- select the task and then click **Run Task**.

The scan window will appear.



An icon will appear in the [system tray](#) when a scan process is running.

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 complexity of the scan.

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.

**Note**

If suspect files were detected during the scan, you will be requested to submit them to the BitDefender Lab.

- **Pause** - stops temporarily the scan process - you can continue it by clicking **Resume**.
- **Show report** - opens the scan report.

**Note**

If you right click a running task, a shortcut (contextual) menu allowing you to manage the scan window will appear. The options (**Pause / Resume**, **Stop** and **Stop&Close**) are similar to those of the buttons in the scan window.

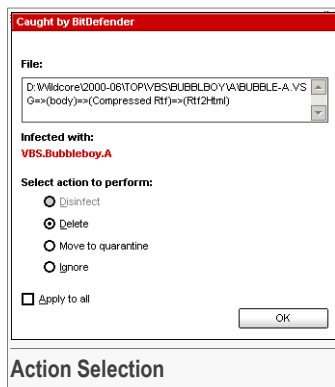
If the **Prompt user for action** option is set in the **Properties** window, when an infected file is detected an alert window will ask you to select the action to be taken on the infected file.

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;
- **Move to quarantine** - moves the infected file into the quarantine;
- **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**

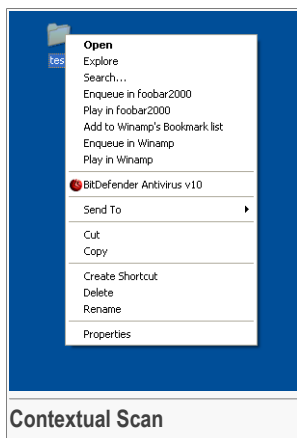
If the **Disinfect** option is not enabled, it means the file cannot be disinfected. The best choice is to isolate it in the quarantine zone and send it to us for analysis or delete it.

Click **OK**.

**Note**

The report file is saved automatically in the [Scan Logs](#) section from the **Properties** window of the respective task.

Contextual Scanning

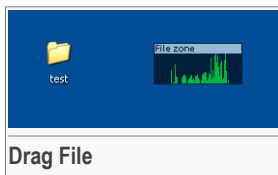


Right-click the file or folder you want scanned and select **BitDefender Antivirus v10**.

You can modify the scan options and see the report files by accessing the [Properties](#) window of the **Contextual Menu Scan** task.

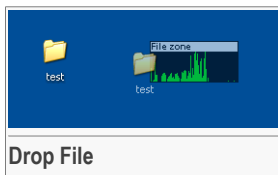
Drag&Drop Scanning

Drag the file or folder you want scanned and drop it over the **Scan Activity Bar** as shown below.



If an infected file is detected an **alert window** will appear asking you to select the action to be taken on the infected file.

In both alternative scanning (contextual and drag&drop scanning) the **scan window** will appear.



7.2.5. Rootkit Scanning

BitDefender comes to solve the latest security threats by introducing a rootkit detector along with its efficient antivirus&antispysware engines. BitDefender is now able to detect rootkits by searching for hidden files, folders or processes. Moreover, it can protect your system by renaming the malware which uses rootkits.

In order to scan your computer for rootkits, run the **Scan for Rootkits** task. A scan window will appear.



Important

When you check for rootkits, it is strongly recommended that you set BitDefender not to take any action on hidden files.

At the end of the scan you can see the results. If hidden files have been detected, check them carefully: the presence of hidden files might indicate a possible intrusion.

If you are sure that the detected files belong to malware, we recommend that you set the **Rename files** action and run the **Scan for Rootkits** task again. In this way, the hidden files will be blocked.



Warning

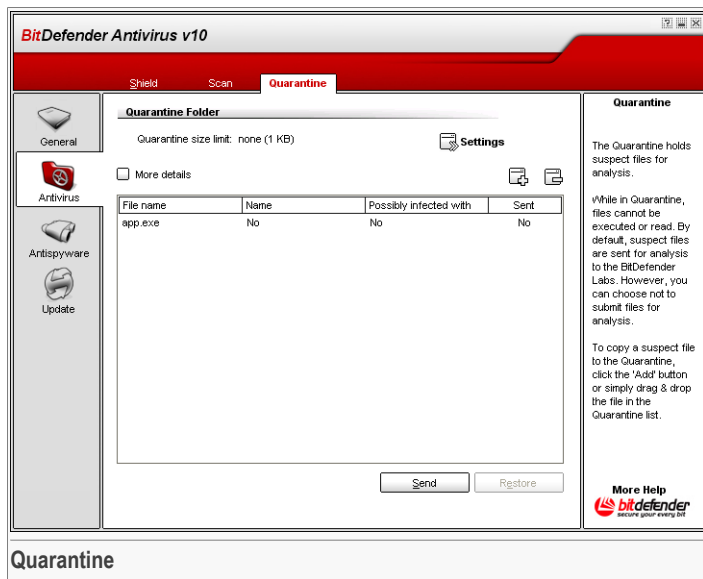
NOT ALL HIDDEN ITEMS ARE MALWARE! Before renaming hidden files, make sure they belong neither to a valid application nor to the system. Renaming such files could render your system unusable.



Important

If your system has been hacked, there is only one safe way of completely doing away with the intrusion: reinstalling the system.

7.3. 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 details**.



Note

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



Click the **Add** button to add 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.

To delete a selected file from quarantine click the **Remove** button. If you want to restore a selected file to its original location click **Restore**.

You can send any selected file from the quarantine to the BitDefender Lab by clicking **Send**.



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.

Click **Settings** to open the advanced options for the quarantine zone. A new window will appear.

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

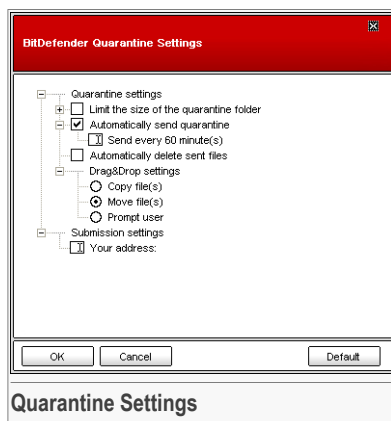
- **Limit the size of quarantine folder** - maintains under control the size of the quarantine. The default size is 12000 kB. If you want to change this value, type a new one in the corresponding field.

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.



Note

By default, the quarantine folder has no size limit.



Quarantine Settings

- **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 every x minutes** 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.



8. Antispyware Module

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

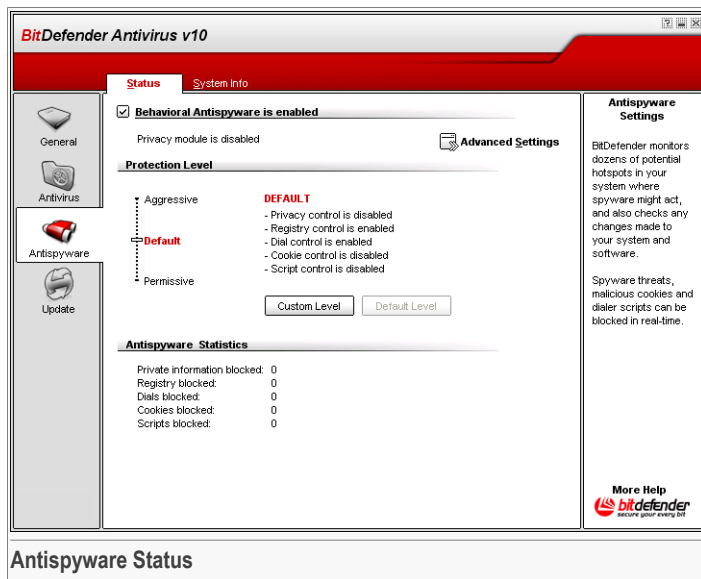
- Antispyware Status
- Advanced Settings - Privacy Control
- Advanced Settings - Registry Control
- Advanced Settings - Dial Control
- Advanced Settings - Cookie Control
- Advanced Settings - Script Control
- System Information

Note



For more details regarding the **Antispyware** module check the description of the *"Antispyware Module"* (p. 25).

8.1. Antispyware Status



In this section you can configure the **Behavioral Antispyware** and you can view information regarding its activity.



Important

To prevent spyware from infecting your computer keep the **Behavioral Antispyware** enabled.

At the bottom of the section you can see the **Antispyware statistics**.

The **Antispyware** module protects your computer against spywares through 5 important protection controls:

- **Privacy Control** - protects your confidential data by filtering all outgoing HTTP and SMTP traffic according to the rules you create in the **Privacy** section.
- **Registry Control** - asks for your permission whenever a program tries to modify a registry entry in order to be executed at Windows start-up.
- **Dial Control** - asks for your permission whenever a dialer attempts to access a computer modem.



- **Cookie Control** - asks for your permission whenever a new website tries to set a cookie.
- **Script Control** - asks for your permission whenever a website tries to activate a script or other active content.

To configure the settings for these controls click  **Advanced Settings**.

8.1.1. Protection Level

You can choose the protection level that better fits your security needs. Drag the slider along the scale to set the appropriate protection level.


There are 3 protection levels:

Protection level	Description
Permissive	Only Registry control is enabled.
Default	Registry control and Dial Control are enabled.
Aggressive	Registry control , Dial Control and Privacy Control are enabled.

You can customize the protection level by clicking **Custom level**. In the window that will appear, select the Antispyware controls you want to enable and click **OK**.


Click **Default Level** to position the slider at the default level.

8.2. Advanced Settings - Privacy Control

To access this section click the  **Advanced Settings** button from the **Antispyware** module, **Status** section.



Whether it is your e-mail or your credit card number, when they fall into the wrong hands such information may cause you damage: you may find yourself drowning in spam messages or you might be surprised to access an emptied account.

The rules must be input manually (click the  **Add** button and choose the parameters for the rule). The configuration wizard will appear.

8.2.1. Configuration Wizard



Step 1/3 - Set Rule Type and Data

BitDefender Wizard Step 1/3

Rule Name:

Rule Type:

Rule Data:

All data you enter is encrypted. For extra safety, do not enter the whole of the data you wish to protect.

< Back Next > Cancel

Set Rule Type and Data

Enter the name of the rule in the edit field.

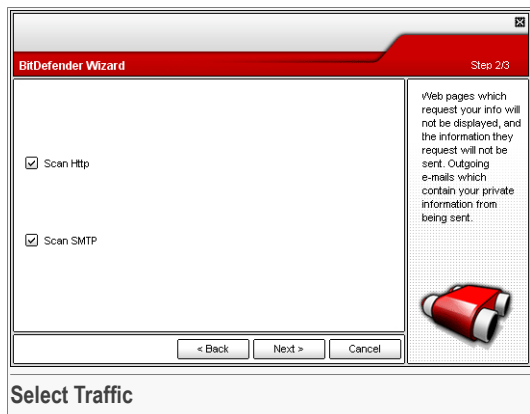
You must set the following parameters:

- **Rule Type** - choose the rule type (address, name, credit card, PIN, SSN etc).
- **Rule Data** - type in the rule data.

All of the data you enter is encrypted. For extra safety, do not enter all of the data you wish to protect.

Click **Next**.

Step 2/3 - Select Traffic



Select the traffic you want BitDefender to scan. The following options are available:

- **Scan HTTP** - scans the HTTP (web) traffic and blocks the outgoing data that matches the rule data.
- **Scan SMTP** - scans the SMTP (mail) traffic and blocks the outgoing e-mail messages that contain the rule data.

Click **Next**.



Step 3/3 - Describe Rule

The image shows a screenshot of the BitDefender Wizard window, specifically Step 3/3 titled "Describe Rule". The window has a red header bar with the text "BitDefender Wizard" on the left and "Step 3/3" on the right. The main area is divided into two sections. On the left, under the heading "Rule Description", there is a text input field containing the text "Banc account". On the right, there is a text area with the instruction: "Enter a description for this rule. The description should help you or other administrators identify what information you blocked with more ease." Below this text area is a small icon of a red and white fire extinguisher. At the bottom of the window, there are three buttons: "< Back", "Finish", and "Cancel". Below the window, the text "Describe Rule" is displayed.

Enter a short description of the rule in the edit field.

Click **Finish**.

8.2.2. Managing the Rules

You can see the rules listed in the table.

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

To edit a rule select it and click the **Edit** button or double-click it. A new window will appear.

Rule Name: Banc account

Rule Type: credit card

Rule data: XXXXXXXXXXXX

☒ Scan http

☒ Scan smtp

Rule Description: Banc account


OK Cancel

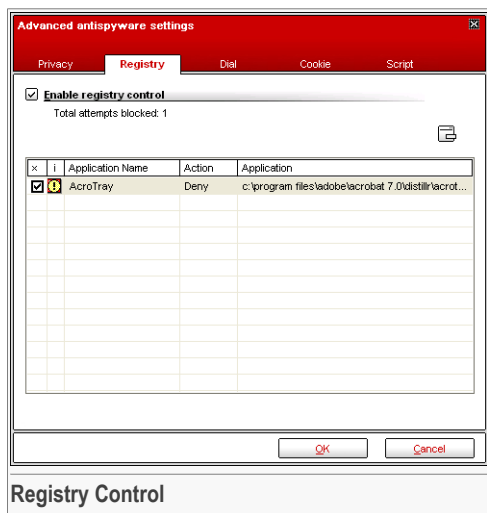
Edit Rule

Here you can change the name, description and parameters of the rule (type, data and traffic). Click **OK** to save the changes.

Click **OK** to save the changes and close the window.

8.3. Advanced Settings - Registry Control

To access this section enter the **Advanced Antispyware Settings** window (go to the **Antispyware** module, **Status** section and click  **Advanced Settings**) and click the **Registry** tab.



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.




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.

To delete a registry entry, just select it and click  **Delete** button. 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

Click **OK** to close the window.

8.4. Advanced Settings - Dial Control


To access this section enter the **Advanced Antispyware Settings** window (go to the **Antispyware** module, **Status** section and click  **Advanced Settings**) and click the **Dial** tab.


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 the  **Delete** button. To modify a parametre of a rule just double click its field and make the desired modification. 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 the  **Add** button and choose the parameters for the rule). The configuration wizard will appear.

8.4.1. Configuration Wizard

The configuration wizard is a 2 steps procedure.

Step 1/2 - 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 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 wild cards 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 **OK** to save the changes and close the window.



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 **Cookie** 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 the  **Delete** button. To modify a parameter of a rule just double click its field and make the desired modification. 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 the  **Add** button and choose the parameters for the rule). The configuration wizard will appear.

8.5.1. Configuration Wizard

The configuration wizard is a 1 step procedure.

Step 1/1 - Select Address, Action and Direction

Select Address, Action and Direction Step 1/1

Enter domain

☐ Any

☒ Enter domain

www.softwin.com

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

Don't show this message again

< Back Finish Cancel

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**.




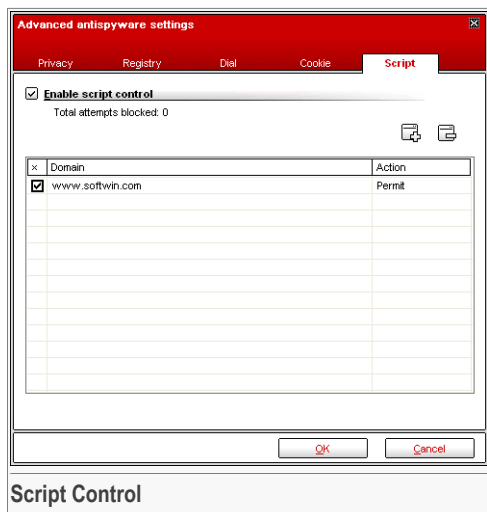
Note

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

Click **OK** to save the changes and close the window.

8.6. Advanced Settings - Script Control

To access this section enter the **Advanced Antispyware Settings** window (go to the **Antispyware** module, **Status** section and click  **Advanced Settings**) and click the **Script** tab.



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:



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 the  **Delete** button. To modify a parametre of a rule just double click its field and make the desired modification. 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 the  **Add** button and choose the parameters for the rule). The configuration wizard will appear.

8.6.1. Configuration Wizard

The configuration wizard is a 1 step procedure.



Step 1/1 - Select Address and Action

Select Address and Action Step 1/1

Enter domain
www.softwin.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 pages will not work if you block scripts.

< Back Finish Cancel

Select Address and Action

You can set the parameters:

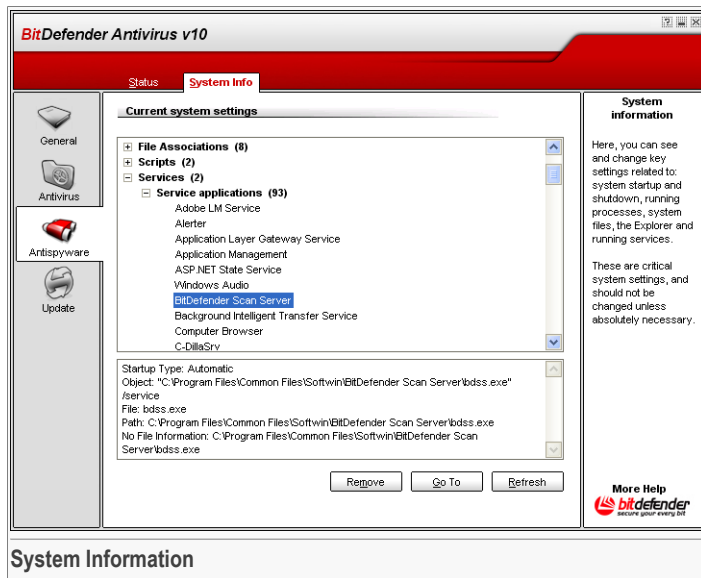
- **Domain address** - type in the domain on which the rule should apply.
- **Action** - select the action of the rule.

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

Click **Finish**.

Click **OK** to save the changes and close the window.

8.7. System Information



Here you can see and change key info settings.

The list contains all the items loaded when starting the system as well as the items loaded by different applications.

Three buttons are available:

- **Remove** - deletes the selected item.
- **Go to** - opens a window where the selected item is placed (the **Registry** for example).
- **Refresh** - re-opens the **System Info** section.



9. 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. 26).

9.1. Automatic Update

BitDefender Antivirus v10

Update Settings

☒ **Automatic update is enabled**

Last checked 3/23/2007 2:37:57 PM
Last updated 3/23/2007 2:38:26 PM

Antivirus signature properties

Virus Signatures 443519
Engine Version 7.12003

Download status

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

Update BitDefender

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.

More Help
 bitdefender
secure your every bit

Automatic Update

In this section you can see update-related information and perform updates.




Important

To be protected against the latest threats keep the **Automatic Update** enabled.

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.

You can get the malware signatures of your BitDefender by clicking  **Show Virus List**. A HTML file that contains all the available signatures will be created. Click again  **Show Virus List** to see the list. You can search through the database for a specific malware signature or click **BitDefender Virus List** to go to the online BitDefender signature database.

9.2. 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.



9.2.1. 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**.

9.2.2. 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 Vista.
- Windows 98, Windows Millennium.

Windows NT-SP6, Windows 2000, Windows XP, Windows Vista

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](#).**

**Note**

If you have Windows Vista installed, you will be requested to confirm most of these actions.

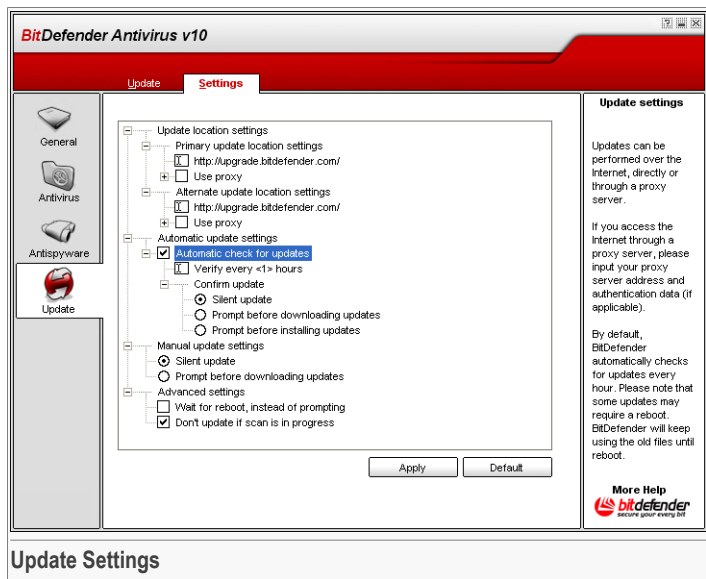
Windows 98, Windows Millennium

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.**



9.3. 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.

9.3.1. 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.

9.3.2. 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.



9.3.3. 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 be 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.

9.3.4. 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



10. Best Practices

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

- [How to Protect Your Computer against Malware Threats](#)
- [How to Configure a Scan Task](#)

10.1. How to Protect Your Computer against Malware Threats

Follow these steps to protect your computer against viruses, spyware and other malware:

1. **Complete the initial setup wizard.** During the installation process a [wizard](#) will appear. It will help you register BitDefender and create a BitDefender account in order to benefit from free technical support. It will also help you set BitDefender to perform important security tasks.



Important

If you have a BitDefender Rescue CD, scan your system before installing BitDefender to ensure that you do not have any malware already existing in your system.

2. **Update BitDefender.** If you have not completed the initial setup wizard during the installation process, perform an update by user request (go to the **Update** module, [Update](#) section, and click **Update Now**).
3. **Perform a full system scan.** Access the **Antivirus** module, [Shield](#) section and click **Scan Now**.



Note

You can also initiate a full system scan from the [Scan](#) section. Select the **Full System Scan** task and click **Run Task**.

4. **Prevent infection.** In the **Shield** section, keep the [real-time protection](#) on in order to be protected against viruses, spyware and other malware. Set the [protection level](#) that best fits your needs. You can [customize](#) it whenever you want by clicking **Custom Level**.

**Important**

Program your BitDefender Antivirus v10 to scan your system at least once a week by [scheduling](#) the **Full System Scan** task from the [Scan](#) section.

5. **Keep your BitDefender current.** In the **Update** module, [Update](#) section, keep the **Automatic Update** enabled in order to be protected against the latest threats.
6. **Schedule a full system scan.** Go to the **Scan** section and program BitDefender to [scan your system](#) at least once a week by [scheduling](#) the **Full System Scan** task.

10.2. How to Configure a Scan Task

Follow these steps to create and configure a scan task:

1. **Create a new task.** Go to the [Scan](#) section and click **New Task**. The [Properties](#) window will appear.

**Note**

You can also create a new task by [duplicating](#) one that already exists. To do this, right-click a task and select **Duplicate** from the shortcut menu. Select the duplicate and click **Properties** to open the **Properties** window.

2. **Set the scan level.** Go to the **Overview** section to set the [scan level](#). If you want, you can [customize](#) the scan settings by clicking **Custom**.
3. **Set the scan target.** Go to the **Scan Path** section and choose the [objects you want to be scanned](#).
4. **Schedule the task.** If the scan task is complex, you might need to schedule it for later, when your computer is in the idle mode. This will help BitDefender perform an accurate scan of your system. Go to the **Scheduler** section to [schedule the task](#).



BitDefender Rescue CD

BitDefender Antivirus v10 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.

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.



11. Overview

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

11.1. 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.”

11.2. 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.

11.3. 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

11.4. 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.

11.4.1. 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.

11.4.2. 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 antispy 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")

11.4.3. 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.



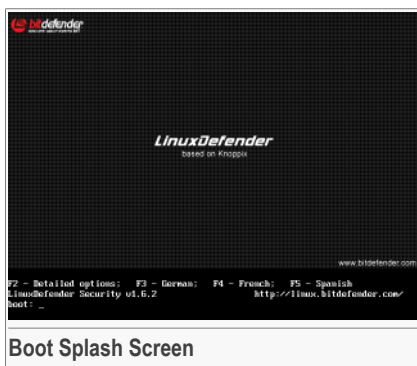
12. LinuxDefender Howto

12.1. Start and Stop

12.1.1. Start LinuxDefender

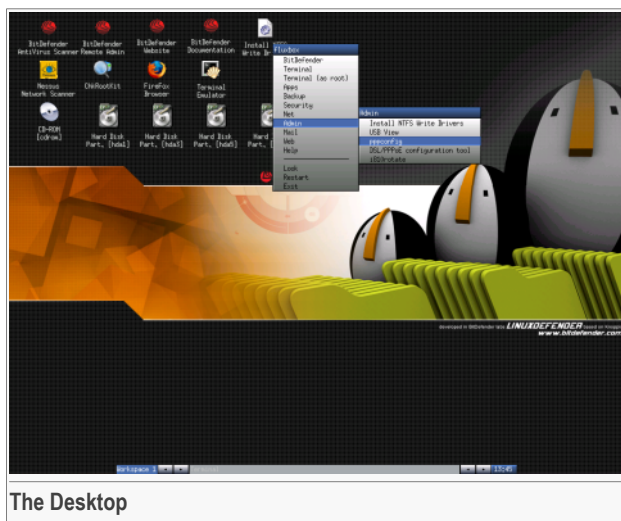
To start the CD, set up the BIOS of your computer to boot off the CD, put the CD in the drive and reboot the computer. Make sure that your computer can boot from CD.

Wait until the next screen shows up and follow the on-screen instructions to start LinuxDefender.



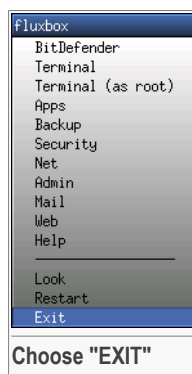
Press **F2** for detailed options. Press **F3** for detailed options in German. Press **F4** for detailed options in French. Press **F5** for detailed options in Spanish. For a quick start-up with default options, just press **ENTER**.

When the boot process has finished you will see the next desktop. You may now start using LinuxDefender.



12.1.2. 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.



When LinuxDefender has successfully 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 unmounted
/randisk unmounted
could not mount /KNOPPIX - trying /dev/cloop instead
/dev/root unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return.
```

Wait for this message when shutting down

12.2. 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.

12.3. 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.

12.4. Virus Scanning

12.4.1. 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).

12.4.2. 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.

12.5. 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.

12.5.1. 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](#).

12.5.2. 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.

12.6. 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.

12.6.1. 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.

12.6.2. Nessus - the Network Scanner

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.

—www.nessus.org

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 network 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.

12.7. 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



13. Support

13.1. Support Department

As a valued provider, BitDefender strives to provide its customers with an unparalleled level of fast and accurate support. The Support Center (which you can contact at the address provided below) continually keeps up with the latest threats. This is where all of your questions are answered in a timely manner.

With BitDefender, 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> at 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.

13.2. On-line Help

13.2.1. 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>.

13.3. 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.

13.3.1. 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>

13.3.2. Branch Offices

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
Headquarter Western Europe
Karlsdorferstrasse 56
88069 Tettnang
Germany
Tel: +49 7542 9444 44
Fax: +49 7542 9444 99
Email: <info@bitdefender.com>
Sales: <sales@bitdefender.com>



Web: <http://www.bitdefender.com>

Technical Support: <support@bitdefender.com>

UK and Ireland

One Victoria Square

Birmingham

B1 1BD

Tel: +44 207 153 9959

Fax: +44 845 130 5069

Email: <info@bitdefender.com>

Sales: <sales@bitdefender.com>

Web: <http://www.bitdefender.co.uk>

Technical support: <support@bitdefender.com>

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 33309

Technical support: <support@bitdefender.com>

Customer Service: 954-776-6262

Web: <http://www.bitdefender.com>

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>



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.

Rootkit

A rootkit is a set of software tools which offer administrator-level access to a system. The term was first used for the UNIX operating systems and it referred to recompiled tools which provided intruders administrative rights, allowing them to conceal their presence so as not to be seen by the system administrators.

The main role of rootkits is to hide processes, files, logins and logs. They may also intercept data from terminals, network connections or peripherals, if they incorporate the appropriate software.

Rootkits are not malicious in nature. For example, systems and even some applications hide critical files using rootkits. However, they are mostly used to hide malware or to conceal the presence of an intruder into the system. When combined with malware, rootkits pose a great threat to the integrity and the security of a system. They can monitor traffic, create backdoors into the system, alter files and logs and avoid detection.

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 its 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.

