

ANTIVIRUS₂₀₀₉

User's guide



Copyright© 2008 BitDefender



BitDefender Antivirus 2009 *User's guide*

Published 2008.10.29

Copyright© 2008 BitDefender

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 BitDefender. 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 BitDefender, therefore BitDefender 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. BitDefender provides these links only as a convenience, and the inclusion of the link does not imply that BitDefender 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

End User Software License Agreement 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
Installation 1
1. System Requirements 2 1.1. Hardware Requirements 2 1.2. Software Requirements 3 2. Installing BitDefender 4 2.1. Registration Wizard 6 2.1.1. Step 1/2 - Register BitDefender Antivirus 2009 7 2.1.2. Step 2/2 - Create a BitDefender Account 8 2.2. Configuration Wizard 10 2.2.1. Step 1/8 - Welcome Window 11 2.2.2. Step 2/8 - Select View Mode 12 2.2.3. Step 3/8 - Configure BitDefender Network 13 2.2.4. Step 4/8 - Configure Identity Control 14 2.2.5. Step 5/8 - Configure Virus Reporting 17 2.2.6. Step 6/8 - Select the Tasks to Be Run 18 2.2.7. Step 7/8 - Wait for the Tasks to Complete 19 2.2.8. Step 8/8 - Finish 20
3. Upgrade 21
4. Repairing or Removing BitDefender 22
Basic Administration 24
5. Getting Started 25 5.1. Start BitDefender Antivirus 2009 25 5.2. User Interface View Mode 25 5.2.1. Basic View 25 5.2.2. Advanced View 27 5.3. BitDefender Icon in the System Tray 30 5.4. Scan Activity Bar 30 5.5. BitDefender Manual Scan 31



 5.6. Game Mode 5.6.1. Using Game Mode 5.6.2. Changing Game Mode Hotkey 5.7. Integration into Web Browsers	32 32 32 33 34
6. Dashboard 6.1. Overview 6.2. Tasks 6.2.1. Scanning with BitDefender 6.2.2. Updating BitDefender	36 91 37 38 38
7. Antivirus 7.1. Monitored Components 7.1.1. Local security 7.2. Tasks 7.2.1. Scanning with BitDefender 7.2.2. Updating BitDefender	40 40 81 42 42 48
 8. Antiphishing	51 51 52 53 53 58
 9. Vulnerability 9.1. Monitored Components 9.1.1. Vulnerability scan 9.2. Tasks 9.2.1. Searching for Vulnerabilities 	61 61 63 63
10. Network 10.1. Tasks 10.1.1. Joining the BitDefender Network 10.1.2. Adding Computers to the BitDefender Network 10.1.3. Managing the BitDefender Network 10.1.4. Scanning All Computers 10.1.5. Updating All Computers 10.1.6. Registering All Computers	70 71 71 71 73 75 76 77
11. Basic Settings 11.1. Local security 11.2. Online security 11.3. General settings	78 79 79 79
12. Status Bar	81



12.2. Online security	. 82
12.3. Vulnerability scan	. 83
13. Registration	85
13.1. Step 1/1 - Register BitDefender Antivirus 2009	. 85
14. History	87
Advanced Administration	89
15. General	90
15.1. Dashboard	. 90
15.1.1. Statistics	. 91
15.1.2. Overview	. 91
15.2. Settings	. 92
15.2.1. General Settings	. 92
15.2.2. Virus Report Settings	. 93
15.3. System Information	. 94
16. Antivirus	. 96
16.1. Real-time Protection	. 96
16.1.1. Configuring Protection Level	. 97
16.1.2. Customizing Protection Level	. 98
16.1.3. Configuring the Behavioral Scanner	102
16.1.4. Disabling Real-time Protection	104
16.1.5. Configuring Antiphishing Protection	105
16.2. On-demand Scanning	106
16.2.1. Scan Tasks	107
16.2.2. Using Shortcut Menu	109
16.2.3. Creating Scan Tasks	110
16.2.4. Configuring Scan Tasks	110
	122
16.2.0. Viewing Scan Logs	129
16.3.1 Excluding Daths from Scapping	130
16.3.2 Excluding Extensions from Scanning	136
16.4 Ouarantine Area	140
16.4.1 Managing Quarantined Files	141
16.4.2. Configuring Quarantine Settings	142
17 Privacy Control	111
17.1 Privacy Control Status	144
17.1.1 Configuring Protection Level	144
17.2 Identity Control	146
17.2.1 Creating Identity Rules	148
17.2.2. Defining Exceptions	151
17.2.3. Managing Rules	152



 17.3. Registry Control 17.4. Cookie Control 17.4.1. Configuration Window 17.5. Script Control 17.5.1. Configuration Window 	153 155 157 159 160
18. Instant Messaging (IM) Encryption 18.1. Disabling Encryption for Specific Users	162 164
19. Vulnerability 19.1. Status 19.1.1. Fixing Vulnerabilities 19.2. Settings	165 165 166 172
20. Game / Laptop Mode	174 175 176 177 178 179 180
21. Network 21.1. Joining the BitDefender Network 21.2. Adding Computers to the BitDefender Network 21.3. Managing the BitDefender Network	181 182 182 184
22. Update 22.1. Automatic Update 22.1.1. Requesting an Update 22.1.2. Disabling Automatic Update 22.2. Update Settings 22.2.1. Setting Update Locations 22.2.2. Configuring Automatic Update 22.2.3. Configuring Manual Update 22.2.4. Configuring Advanced Settings 22.2.5. Managing Proxies	187 189 189 190 191 191 192 192 192
23. Registration 23.1. Registering BitDefender Antivirus 2009 23.2. Creating a BitDefender Account	195 195 197
Getting Help	200
24.1. BitDefender Knowledge Base	201 201



24.2. Asking for Help	202
24.2.1. Go to Web Self Service	202
24.2.2. Open a support ticket	202
24.3. Contact Information	203
24.3.1. Web Addresses	203
24.3.2. Branch Offices	203
BitDefender Rescue CD	206
25. Overview	207
25.1. System Requirements	207
25.2. Included Software	208
26. BitDefender Rescue CD Howto	211
26.1. Start BitDefender Rescue CD	211
26.2. Stop BitDefender Rescue CD	212
26.3. How do I perform an antivirus scan?	213
26.4. How do I configure the Internet connection?	214
26.5. How do I update BitDefender?	215
26.5.1. How do I update BitDefender over a proxy?	216
26.6. How do I save my data?	216
Glossary	219



End User Software License Agreement

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.

PRODUCT REGISTRATION. By accepting this Agreement, You agree to register Your Software, using "My account", as a condition of Your use of the Software (receiving updates) and Your right to Maintenance. This control helps ensure that the Software operates only on validly licensed Computers and that validly licensed end users receive Maintenance services. Registration requires a valid product serial number and a valid email address for renewal and other legal notices.

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 BITDEFENDER for use of BITDEFENDER'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. BITDEFENDER 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.

EXPIRATION. The product will cease to perform its functions immediately upon expiration of the license.

UPGRADES. If BitDefender is labeled as an upgrade, you must be properly licensed to use a product identified by BITDEFENDER 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 BITDEFENDER 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 BITDEFENDER. 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. BITDEFENDER 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 BITDEFENDER, at its option, may replace the defective media upon receipt of the damaged media, or refund the money you paid for BitDefender. BITDEFENDER does not warrant that BitDefender will be uninterrupted or error free or that the errors will



be corrected. BITDEFENDER does not warrant that BitDefender will meet your requirements.

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, BITDEFENDER 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. BITDEFENDER 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 BITDEFENDER 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 BITDEFENDER 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 BITDEFENDER'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.

CONSENT TO ELECRONIC COMMUNICATIONS. BitDefender may be required to send you legal notices and other communications about the Software and Maintenance subscription services or our use of the information you provide us ("Communications").



BitDefender will send Communications via in-product notices or via email to the primary user's registered email address, or will post Communications on its Sites. By accepting this Agreement, you consent to receive all Communications through these electronic means only and acknowledge and demonstrate that you can access Communications on Sites.

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 BITDEFENDER. 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 BITDEFENDER 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.

BITDEFENDER 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 BITDEFENDER shall prevail.

Contact BITDEFENDER, at 24, Preciziei Boulevard, West Gate Building H2, ground floor, Sector 6, Bucharest, Romania, or at Tel No: 40-21-206.34.70 or Fax: 40-21-264.17.99, e-mail address: office@bitdefender.com.



Preface

This guide is intended to all users who have chosen **BitDefender Antivirus 2009** 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 2009**, 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 2009**, how to update, test and customize it. You will learn how to get best from BitDefender.

We wish you a pleasant and useful lecture.

1. Conventions Used in This Book

1.1. Typographical Conventions

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

Appearance	Description
sample syntax	Syntax samples are printed with monospaced characters.
http://www.bitdefender.com	The URL link is pointing to some external location, on http or ftp servers.
support@bitdefender.com	E-mail 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 monospaced font.
option	All the product options are printed using strong characters.
sample code listing	The code listing is printed with monospaced characters.



1.2. Admonitions

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



Note

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



Important

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



Warning

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

2. The Book Structure

The book consists of several parts containing major topics. Moreover, a glossary is provided to clarify some technical terms.

Installation. Step by step instructions for installing BitDefender on a workstation. This is a comprehensive tutorial on installing **BitDefender Antivirus 2009**. 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.

Basic Administration. Description of basic administration and maintenance of BitDefender.

Advanced Administration. A detailed presentation of the security capabilities provided by BitDefender. You are taught how to configure and use all BitDefender modules so as to efficiently protect your computer against all kind of malware threats (viruses, spyware, rootkits and so on).

Getting Help. Where to look and where to ask for help if something unexpected appears.

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



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.



Important

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



Installation



1. System Requirements

You may install BitDefender Antivirus 2009 only on computers running the following operating systems:

- Windows XP with Service Pack 2 (32/64 bit) or higher
- Windows Vista (32/64 bit) or Windows Vista with Service Pack 1
- Windows Home Server

Note

Before installation, make sure that your computer meets the minimum hardware and software requirements.



To find out the Windows operating system your computer is running and hardware information, right-click **My Computer** on the desktop and then select **Properties** from the menu.

1.1. Hardware Requirements

For Windows XP

- 800 MHz or higher processor
- 256 MB of RAM Memory (1GB recommended)
- 170 MB available hard disk space (200 MB recommended)

For Windows Vista

- 800 MHz or higher processor
- 512 MB of RAM Memory (1 GB recommended)
- 170 MB available hard disk space (200 MB recommended)

For Windows Home Server

- 800 MHz or higher processor
- 512 MB of RAM Memory (1 GB recommended)
- 170 MB available hard disk space (200 MB recommended)



1.2. Software Requirements

- Internet Explorer 6.0 (or higher)
- .NET Framework 1.1 (also available in the installer kit)

Antiphishing protection is provided only for:

- Internet Explorer 6.0 or higher
- Mozilla Firefox 2.0
- Yahoo! Messenger 8.1
- Windows Live (MSN) Messenger 8.5

Instant Messaging (IM) encryption is provided only for:

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



2. Installing BitDefender

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

Before launching the setup wizard, BitDefender will check for newer versions of the installation package. If a newer version is available, you will be prompted to download it. Click **Yes** to download the newer version or **No** to continue installing the version then available in the setup file.





Follow these steps to install BitDefender Antivirus 2009:

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

BitDefender Antivirus 2009 alerts you if you have other antivirus products installed on your computer. Click **Remove** to uninstall the corresponding product. If you want to continue without removing the detected products, click **Next**.



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.

3. Please read the License Agreement and click I agree.



Important

If you do not agree to these terms click **Cancel**. The installation process will be abandoned and you will exit setup.

4. By default, BitDefender Antivirus 2009 will be installed in C:\Program Files\BitDefender\BitDefender 2009. If you want to change the installation path, click **Browse** and select the folder in which you would like BitDefender to be installed.

Click Next.

- 5. Select options regarding the installation process. Some of them will be 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 2009 on your desktop at the end of the installation.
 - Eject CD when installation is complete to have the CD ejected at the end of the installation; this option appears when you install the product from the CD.
 - 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. If not already installed, BitDefender will first install .NET Framework 1.1.

Wait until the installation is completed.



6. Click **Finish**. You will be asked to restart your system so that the setup wizard can complete the installation process. We recommend doing so as soon as possible.



Important

After completing the installation and restarting the computer, a registration wizard and a configuration wizard will appear. Complete these wizards in order to register and configure BitDefender Antivirus 2009 and to create a BitDefender account.

If you have accepted the default settings for the installation path, you can see in Program Files a new folder, named BitDefender, which contains the subfolder BitDefender 2009.

2.1. Registration Wizard

The first time you start your computer after installation, a registration wizard will appear. The wizard helps you register BitDefender and configure a BitDefender account.

You MUST create a BitDefender account in order to receive BitDefender updates. The BitDefender account also gives you access to free technical support and special offers and promotions. If you loose your BitDefender license key, you can log in to your account at http://myaccount.bitdefender.com to retrieve it.



Note

If you do not want to follow this wizard, click **Cancel**. You can open the registration wizard anytime you want by clicking the **Register** link, located at the bottom of the user interface.



2.1.1. Step 1/2 - Register BitDefender Antivirus 2009

tberender Registration wizard	1- Step I OF Z	
Step 1		Step 2
Welcome to the BitDefender Registration	n Wizard!	This is where you can find your
This wizard will help you register BitDefender and Account	create or update your BitDefender	license key: 1) CD-Rom label
Your current BitDefender license status is:	Trial	Serie de lovegintere: 3030300000000000000000000000000000000
Your current BitDefender license key is:	704BE277EF7785580DF8	
This license key will expire in:	30 days	2
Licensing Options		2) Product registration card
If you want to keep the current key, please selenew key, please select the second option and fill	ct the first option. If you want to add a the key in the box below.	
Continue using the current key		
 I want to register the product with a new key 	/	Online purchase e-mail
Enter a new license key:		C A. A. J A. A. J
Buy a license key		Barla da loregidatura 2005 SESESES SESESESESESESESESESESESESESESE
If you want to buy a license key, please visit ou	r online store at:	
Renew Your BitDefender license Key		internet in an and a second seco
2		
Shitdefender (State)		Pack Neut Cancal

You can see the BitDefender registration status, the current license key and how many days are left until the license expires.

To continue evaluating the product, select **Continue using the current key**.

To register BitDefender Antivirus 2009:

1. Select I want to register the product with a new key.

2. Type the license key in the edit field.



Note

You can find your license key:

- on the CD label.
- on the product registration card.
- in the online purchase e-mail.



If you do not have a BitDefender license key, click the provided link to go to the BitDefender online store and buy one.

Click Next to continue.

2.1.2. Step 2/2 - Create a BitDefender Account

Step 1	Step 2
In Account registration formation about an existing BitDefender account was found o pecial offers and promotions. If you lose your BitDefender lice noose to sign in to an existing BitDefender Account or to creat	on this computer. The BitDefender Account gives you access to technical support a nese key you can retrieve it by logging in to http://myaccount.bitdefender.com. You te a new one.
) Sign in to an existing BitDefender Account	Create a new BitDefender Account
E-mail address:	E-mail Address: vdanciu@yahoo.com
Password:	Password: *********
Forgot your password?	Re-Type password: *********
	First Name: Cosmin
	Last Name
	Country: Jointed States
Skip registration	
	Send me all messages from BitDefender
	Send me only the most important messages
	O Don't send me any messages
2	

If you do not want to create a BitDefender account at the moment, select **Skip** registration and click **Finish**. Otherwise, proceed according to your current situation:

- "I do not have a BitDefender account" (p. 9)
- "I already have a BitDefender account" (p. 9)



Important

You must create an account within 15 days after installing BitDefender (if you register it, the deadline is extended to 30 days). Otherwise, BitDefender will no longer update.



I do not have a BitDefender account

To create a BitDefender account, select **Create a new BitDefender account** and provide the required information. The data you provide here will remain confidential.

- **E-mail address** type in your e-mail address.
- Password type in a password for your BitDefender account. The password must be at least six characters long.
- **Re-type password** type in again the previously specified password.
- First name type in your first name.
- **Last name** type in your last name.
- **Country** select the country you reside in.



Note

Use the provided e-mail address and password to log in to your account at http://myaccount.bitdefender.com.

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.

Optionally, BitDefender can inform you about special offers and promotions using the e-mail address of your account. Select one of the available options:

- Send me all messages from BitDefender
- Send me only the most important messages
- Don't send me any messages

Click Finish.

I already have a BitDefender account

BitDefender will automatically detect if you have previously registered a BitDefender account on your computer. In this case, provide the password of your account.

If you already have an active account, but BitDefender does not detect it, select **Sign in to an existing BitDefender Account** and provide the e-mail address and the password of your account.

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



Optionally, BitDefender can inform you about special offers and promotions using the e-mail address of your account. Select one of the available options:

- Send me all messages from BitDefender
- Send me only the most important messages
- Don't send me any messages

Click Finish.

2.2. Configuration Wizard

Once you have completed the registration wizard, a configuration wizard will appear. The wizard helps you configure specific product modules 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 2009 is installed.



Note

If you do not want to follow this wizard, click **Cancel**. BitDefender will notify you about the components that you need to configure when you open the user interface.



2.2.1. Step 1/8 - Welcome Window

Bit Defende	er Antivir	us 2	009								-	1
3itDefender (Configurat	ion W	/izard -	Ste	p 1 of 8							
Step 1	Step 2		Step 3		Step 4	Step	5	Step 6	S	tep 7	Step 8	
Welcome to the	BitDefender (Config	uration W	/izard	li							
This wizard will guid - configure the mos - apply the settings - take the first actio	e you through t t important BitD that will best co ons towards mal	the step refender over you king you	s necessar r modules ur requirem ir computer	ry for y nents a r virus	you to: and security r -free.	needs						
If this is the first tin 'Next'. You can skip product, you will be	ne you install Bit the wizard alto notified to con	Defend gether figure it	er it is reco and start u s compone	ommen Ising B nts.	ided to proce itDefender wi	ed with this (thout any cu	vizard. Y Istomized	'ou can also choc d configuration. F	se to skip łowever,	o any of its once you:	steps by clickin start using the	ıg
You can notify yo	choose to sk ou that you n	ip this eed to	wizard's configur	steps re its	s and start component	using BitD s.	efender	r not configure	ed. How	ever, the	e product will	1
Click Next to sta	rt configuring your	BitDefe	nder product.									
ei.												
Solit defende	r							Back		Next	Canc	el



2.2.2. Step 2/8 - Select View Mode

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8
er Interface V	iew Mode						
can chose to vie	v BitDefender u	nder Basic or Adva	anced mode depe	nding on your user	experience with ou	ur product	
Basic View				O Advance	d View		
imple Interface t asic level. You'll lerts and fix und	hat will give you have to keep tra esired issues	u access to all modi ack of warnings an	ules at a d critical	Advanced component advanced	interface that gives of BitDefender pro settings as well as k	you access to each s duct. You'll be able to eep track of advance	pecific configure d features
Defender Total Security 2005	C. C			Di/Defender Tota	i Security 2009 - Beta	and a second	
	0 ⁰ 0 0			MATEL there is 3 pe	DeMored Server Server	FEE ALL DIVIDE	
Buthites	Oversiew	Tasks		Antonia Antonia	Statistics Scanned New 1237	Overview 5 Last spilate Serve	
In anned Hins. Datafected Hins. Debuted viewens:	1 Lad splater 5/10 1 Hylecounti 1 Replations	No mineri No mineri No mineri S, Deep Scan		Parential Control Broady Control	Delected New Delected viewers	0 Maylocousti Issuntrification.com 0 Registration: Initiation	
Washed part acare Completed backup jobs:	fogiero in	II days laft		Present National data	Bicked part scarse Completed backup pilos Effectores	0 Explores inc	
				theraption Transp		- Core	
				Modult Trends Network	11.0	يا باليدية المحيد	
Q. Phone distribution on our first difficult control of a set of the set o	dik u ordgen u ded aak d'te orgenatis. Billeb	linis of anatise is up a factor in an inc.		Tophts Neght aton and Topport			
u Midelandar	Be - Bu	nunet - beate - tek - baset - telog					
				0			
				@bildefunder		Bohumet - Bearlet - 1986 - Barret - 1986	×.
You'll be a	ble to switch	between these	: views at any	moment when u	ising BitDefende	r	

Choose between the two user interface view modes depending on your user experience with BitDefender:

- Basic View. Simple interface suited for beginners and users who want to perform basic tasks and easily solve problems. You just have to keep track of the BitDefender warnings and alerts and fix the issues that appear.
- Advanced View. Advanced interface suited for more technical users who want to fully configure the product. You can configure each product component and perform advanced tasks.



2.2.3. Step 3/8 - Configure BitDefender Network

t Defender Antivi	rus 2009							-
tDefender Configura	tion Wizard	- Step	3 of 8					
Step 1 Step 2	Step 3	S	tep 4	Step 5	Step 6	Step 7		Step 8
ome Management Configur	ation							
tDefender 2009 includes a new nd to manage all of the BitDefen art of a network created and ma	module, Home Man der products instal naged from anothe	agement, lled in this er computi	which enable: network. You er.	s you to create a can act as an ac	a virtual network of a Iministrator of a net	all the compute work that you	ers in your create or	household you can be
lick the check box below if you w	ant to be part of t	he BitDefe	nder Home Ne	etwork. You will t	be required to enter	a Home Mana	gement pa	assword
nich will allow the administrator	or your network to	control th	e bitverender	settings and act	tions on this comput	er remotely.		
I want to be a part of the BitDe	fender Home Netv	vork						
		k in a k in		_				
ome Management password:	*****							
ome Management password:	*******	ka kad		_				
lome Management password: e-type password:	*******	****						
lome Management password: e-type password:	*******	****						
iome Management password: .e-type password:	*******	****						
lome Management password: .e-type password:	*******	****						
lome Management password: e-type password:	*******	****		-				
ome Management password: e-type password:	******	****		_				
ome Management password: e-type password:	****	****						
lome Management password: e-type password:	******	****		-				
ome Management password: e-type password:	*****	****						

BitDefender Network Configuration

BitDefender enables you to create a virtual network of the computers in your household and to manage the BitDefender products installed in this network.

If you want this computer to be part of the BitDefender Home Network, follow these steps:

1. Select I want to be a part of the BitDefender Home Network.

2. Type the same administrative password in each of the edit fields.



Important

The password enables an administrator to manage this BitDefender product from another computer.

2.2.4. Step 4/8 - Configure Identity Control

<mark>it</mark> Defende	r Antivirus	2009						-
itDefender C	onfiguratior	ı Wizard	- Step	4 of 8				
Step 1	Step 2	Step 3	1	itep 4	Step 5	Step 6	Step 7	Step 8
Manage Identity	Rules Page							
The BitDefender Ide redit card number,	ntity Control modu e-mail address, etr	ile helps you :.	keep your	confidentia	al data safe and it p	protects you against	the theft of sensitive da	ta such as y
t will also help you n use this module, you under your account	naintain the confid I need to enable ar credentials.	entiality of y nd configure	our data b Identity co	y scanning ontrol. All in	all web and e-mail formation that you	traffic for specific st I enter here will be e	rings. In order to ncrypted with	
I want to use Ider	itity Control						Add Re	move
Rule Name	Rule Type	HTTP	SMTP	IM	Whole words	Mach Case	Description	
Credit Card Nu	Credit card	YES	YES	NO	YES	NO	My credit card num	ber
							Ежс	eptions
⊇ ≥bitdefende	P					Pack] Next	Cancel

Identity Control protects you against the theft of sensitive data when you are online. Based on the rules you create, Identity Control scans the web, e-mail and instant messaging traffic leaving your computer for specific character strings (for example, your credit card number). If there is a match, the respective web page, e-mail or instant message is blocked.

If you want to use Identity Control, follow these steps:

- 1. Select I want to configure it now.
- 2. Create rules to protect your sensitive data. For more information, please refer to "Creating Identity Control Rules" (p. 15).
- 3. If needed, define specific exceptions to the rules you have created. For more information, please refer to "Defining Identity Control Exceptions" (p. 16).



Creating Identity Control Rules

To create an Identity Control rule, click Add. The configuration window will appear.

Add Ide	entity Rule	x
Rule Name	Credit Card Number	Scan HTTP
Rule Type	Credit card	Mach Whole Words
Rule Data	123412341234	Can Instant Messanging
Inly credit	card number	
Q		

Identity Control Rule

You must set the following parameters:

- **Rule Name** type the name of the rule in this edit field.
- **Rule Type** choose the rule type (address, name, credit card, PIN, SSN etc).
- Rule Data type the data you want to protect in this edit field. For example, if you want to protect your credit card number, type all or part of it here.



Note

If you enter less than three characters, you will be prompted to validate the data. We recommend you to enter at least three characters in order to avoid the mistaken blocking of messages and web pages.

You can choose to apply the rule only if the rule data matches whole words or if the rule data and the detected string case match.

In order to easily identify the information the rule blocks, provide a detailed rule description in the edit box.

To specify the type of traffic to scan, configure these options:



- 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.
- **Scan Instant Messaging** scans the Instant Messaging traffic and blocks the outgoing chat messages that contain the rule data.

Click **OK** to add the rule.

Defining Identity Control Exceptions

There are cases when you need to define exceptions to specific identity rules. Let's consider the case when you create a rule that prevents your credit card number from being sent over HTTP (web). Whenever your credit card number is submitted on a website from your user account, the respective page is blocked. If you want, for example, to buy footwear from an online shop (which you know to be secure), you will have to specify an exception to the respective rule.

Add Exception		×
Allowed Web/e-mail address	Exception Type	
Specify allowed address	HTTP	

To open the window where you can manage exceptions, click **Exceptions**.

I de máiter d	Control	Eveentione	
identity (CONTROL	Exceptions	

To add an exception, follow these steps:

- 1. Click the Add button to add a new entry in the table.
- 2. Double-click **Specify allowed address** and provide the web address or the mail address that you want to add as exception.

Q



- 3. Double-click **Choose type** and choose from the menu the option corresponding to the type of address previously provided.
 - If you have specified a web address, select HTTP.
 - If you have specified an e-mail address, select SMTP.

To remove an exception, select it and click the **Remove** button.

Click OK to close the window.

2.2.5. Step 5/8 - Configure Virus Reporting



BitDefender can send to the BitDefender Labs anonymous reports regarding viruses found on your computer in order to keep track of virus outbreaks.

You can configure the following options:

Send virus reports - send to the BitDefender Labs reports regarding the viruses identified in your computer.



Enable BitDefender Outbreak Detection - send to the BitDefender Labs reports regarding potential virus-outbreaks.



Note

The reports will contain no confidential data, such as your name or IP address, and they will not be used for commercial purposes.

Click Next to continue.

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



Set BitDefender Antivirus 2009 to perform important tasks for the security of your system. The following options are available:

Update the BitDefender engines (may require reboot) - during the next step, an update of the BitDefender 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 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.

Click Next to continue.

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

Bi	Bit Defender Antivirus 2009 -							
Bi	BitDefender Configuration Wizard - Step 7 of 8							
	Step 1	Step 2 Step	p 3 Step 4	4 Step 5	Step 6	Step 7	Step 8	
BI	tverender updati	e						
	BitDefender Upda	te process failed (ur	nable to update or	process canceled).				
	File:		0%		0 kb			
					3			
	Total Update:		0%		0 kb			
F	2							
C	1							
Ľ	bitdefender				Back	Next	Cancel	
Газ	sk Status							

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.

2.2.8. Step 8/8 - Finish

Bit Defender Antiviru	ıs 2009					_ ×
BitDefender Configuratio	on Wizard - S	tep 8 of 8				
Step 1 Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8
Finish						
Thank you for using BitDefender Tot BitDefender Account and the expirin	al Security 2009. Ple g date of the currer	ease refer to the Re It license key.	gister button in I	the main window of	the product for infor	nation on your
During the last 30 days of your BitDe To purchase a new BitDefender key	efender license, the please refer to the f	number of days left Buy button available	until expiration in the same win	will be displayed in t dow.	he dashboard inside	:he main console.
BRDefender Total Security 2009 has been configured. To launch the product, double click the BRDefender red icon in the systray menu. In basic view mode, the dashboard from the main window displays the overall protection status and critical issues that require your attention. For advanced options, click Switch to Advanced View in the same window.						
Open my BitDefender Account (Ir	nternet connection r	equired)				
Q						
(Spitdefender)				Back	Finish	Cancel
inish						

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

Click Finish.



3. Upgrade

In order to upgrade an older version of BitDefender to BitDefender Antivirus 2009, follow these steps:

- 1. Remove the older version of BitDefender from your computer. For more information, please refer to the help file or user manual of the product.
- 2. Restart the computer.
- 3. Install BitDefender Antivirus 2009 as described in the "*Installing BitDefender*" (p. 4) section of this user guide.


4. Repairing or Removing BitDefender

If you want to repair or remove **BitDefender Antivirus 2009**, follow the path from the Windows start menu: **Start** \rightarrow **Programs** \rightarrow **BitDefender 2009** \rightarrow **Repair or Remove**.

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

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

If you choose to repair BitDefender, a new window will appear. Click **Repair** to start the repairing process.

Restart the computer when prompted and, afterwards, click **Install** to reinstall BitDefender Antivirus 2009.

Once the installation process is completed, a new window will appear. Click Finish.

Remove - to remove all installed components.



Note

We recommend that you choose **Remove** for a clean re-installation.

If you choose to remove BitDefender, a new window will appear.



Important

Windows Vista only! By removing BitDefender, you will no longer be protected against malware threats, such as viruses and spyware. If you want Windows Defender to be enabled after uninstalling BitDefender, select the corresponding check box.

Click Remove to start the removal of BitDefender Antivirus 2009 from your computer.

During the removal process you will be prompted to give us your feedback. Please click **OK** to take an online survey consisting of no more than five short questions. If you do not want to take the survey, just click **Cancel**.

Once the removal process is completed, a new window will appear. Click Finish.



Note

After the removal process is over, we recommend that you delete the <code>BitDefender</code> folder from <code>Program Files</code>.



An error occurred while removing BitDefender

If an error has occurred while removing BitDefender, the removal process will be aborted and a new window will appear. Click **Run UninstallTool** to make sure that BitDefender has been completely removed. The uninstall tool will remove all the files and registry keys that were not removed during the automatic removal process.



Basic Administration



5. Getting Started

Once you have installed BitDefender your computer is protected.

5.1. Start BitDefender Antivirus 2009

The first step in getting the best from the BitDefender is to start the application.

To access the BitDefender Antivirus 2009 main interface, use the Windows Start menu, by following the path Start \rightarrow Programs \rightarrow BitDefender 2009 \rightarrow BitDefender Antivirus 2009 or quicker, double click the **Start Formula** BitDefender icon in the system tray.

5.2. User Interface View Mode

BitDefender Antivirus 2009 meets the need of either very technical people or computer beginners. So, the graphical user interface is designed to suit each and every category of users.

You can chose to view BitDefender under Basic or Advanced mode depending on your user experience with our product.



Note

You can easily select one of these windows by clicking, respectively, the **Switch to Basic View** button or the **Switch to Advanced View** button.

5.2.1. Basic View

Basic View is a simple interface that gives you access to all modules at a basic level. You'll have to keep track of warnings and critical alerts and fix undesired issues.

BitDefender Antivirus 2009 - Trial			SETTINGS SWITCH TO ADVANCED VIEW	
STATUS: There are 2 pe	nding issues			FIX ALL ISSUES
DASHBOARD	ANTIVIRUS CRITICAL WARNING	ANTIPHISHING PROTECTED	VULNERABILITY PROTECTED	NETWORK
				Tasks
				→ Full System Scan
CRITICAL WARNING				→ Deep Scan
				 Update Now
There are 2 issues that affective of the contract of the contr	ect your system's security.		FIX ALL ISSUES	
Registration:		Last update:	Never	
Expires in:		Last scan:	Never	
	30 days left	Next scan:	Never	
Q				
(Spitdefender)			My Account - Register	- <u>Help</u> - <u>Support</u> - <u>History</u>
Basic View				

As you can easily notice, in the upper part of the window there are two buttons and a status bar.

ltem	Description
Settings	Opens a windows where you can easily enable or disable important security modules.
Switch to Advanced View	Opens the Advanced View window. This is where you can see the full list of modules and to be able to configure in detail each of the component. The BitDefender will remember this option the next time you will open the user interface.
Status	Contains information about and helps you fix the security vulnerabilities of your computer.

In the middle of the window there are five tabs.



Tab	Description
Dashboard	Displays meaningful product statistics and your registration status together with links to the most important on-demand tasks.
Antivirus	Displays the status of the antivirus module that helps you keep your BitDefender up to date and your computer virus free.
Antiphishing	Displays the status of the antiphishing module that ensures that all web pages access by you via Internet Explorer or Firefox are safe.
Vulnerability	Displays the status of the vulnerability module that helps you keep crucial software on your PC up-to-date.
Network	Displays the BitDefender home network structure.

Furthermore, the BitDefender Basic View window contains several useful shortcuts.

Link	Description
My Account	Allows you to create or to login to your BitDefender account. BitDefender account provides you free access to technical support.
Register	Allows you to enter a new license key or to view the current license key and the registration status.
Help	Gives you access to a help file that learn you how to use BitDefender.
Support	Allows you to contact the BitDefender support team.
History	Allows you to see a detailed history of all tasks performed by BitDefender on your system.

5.2.2. Advanced View

Advanced View gives you access to each specific component of BitDefender product. You'll be able to configure advanced settings as well as keep track of advanced features.

<mark>Bit</mark> Defender Antiv	irus 2009 - Trial		SWITC	TH TO BASIC VIEW
STATUS: There is 1 pen	ding issue			FIX ALL ISSUES
	Dashboard Settings	SysInfo		
ieneral				
ntivirus	Statistics		Overview	
rivacy Control	Scanned files:	3593	Last update:	7/17/2008 4:08 PM
ulnerability	Disinfected files:	0	MyAccount:	No account
ncryption	Detected viruses:	0	Registration:	trial version
etwork			Expires in:	
odate	_			30 days left
egistration	Filezone			
0				
e 1				
Sitdefender			My Account - Registe	r - Help - Support - History
dvanced View				

As you can easily notice, in the upper part of the window there are a button and a status bar.

ltem	Description
Switch to Basic View	Opens the Basic View window. This is where you can see the basic BitDefender interface including the main modules (Security, Tune-Up, File Manager, Network) and a dashboard. The BitDefender will remember this option the next time you will open the user interface.
Status	Contains information about and helps you fix the security vulnerabilities of your computer.

• On the left side of the window there is a menu containing all security modules.



Module	Description
General	Allows you to access the general settings or to view the dashboard and detailed system info.
Antivirus	Allows you to configure your virus shield and scanning operations in detail, to set exceptions and to configure the quarantine module.
Privacy Control	Allows you to prevent data theft from your computer and protect your privacy while you are online.
Encryption	Allows you to encrypt Yahoo and Windows Live (MSN) Messenger communications.
Vulnerability	Allows you to keep crucial software on your PC up-to-date.
Game/Laptop Mode	Allows you to postpone the BitDefender scheduled tasks while your laptop runs on batteries and also to eliminate all alerts and pop-ups when you are playing.
Network	Allows you to configure and manage several computers in your household.
Update	Allows you to obtain info on the latest updates, to update the product and to configure the update process in detail.
Registration	Allows you to register BitDefender Antivirus 2009, to change the license key or to create a BitDefender account.

 Furthermore, the BitDefender Advanced View window contains several useful shortcuts.

Link	Description
My Account	Allows you to create or to login to your BitDefender account. BitDefender account provides you free access to technical support.
Register	Allows you to enter a new license key or to view the current license key and the registration status.
Help	Gives you access to a help file that learn you how to use BitDefender.
Support	Allows you to contact the BitDefender support team.



Link

Description

History

Allows you to see a detailed history of all tasks performed by BitDefender on your system.

5.3. BitDefender Icon in the System Tray

To manage the entire product more quickly, you can also use the BitDefender Icon in the System Tray.

If you double-click this icon, the BitDefender will open. Also, by right-clicking the icon, a contextual menu will allow you to quickly manage the BitDefender product.

- Show opens the BitDefender.
- Help opens the help file that explained the BitDefender Antivirus 2009 in detail.
- About opens the BitDefender web page.
- Fix all issues helps you remove security vulnerabilities.
- Turn on / off Game Mode turns Game Mode on / off.
- Update now starts an immediate update. A new window will appear where you can see the update status.
- Basic settings allows you to easily enable or disable important security modules. A new window will appear where you can activate / inactivate them with a simple click.

While in Game Mode, you can see the letter G over the @ BitDefender icon.

If there are critical issues affecting the security of your system, an exclamation mark is displayed over the A BitDefender icon. You can hover the mouse over the icon to see the number of issues affecting the system's security.

5.4. Scan Activity Bar

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



BitDefender Icon



The gray 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 real-time protection is disabled by displaying a red cross over the **File Zone**.



You can use the **Scan activity bar** to scan objects. Just drag the objects that you want to be scanned and drop them over it. For more information, please refer to "*Drag&Drop Scanning*" (p. 123).

When you no longer want to see the graphic visualization, just right-click it and select **Hide**. To completely hide this window, follow these steps:

- 1. Click Switch to Advanced View (if you are in Basic View).
- 2. Click the General module from the left side menu.
- 3. Click the Settings tab.
- 4. Clear the Enable the Scan Activity bar (on screen graph of product activity) check box.

5.5. BitDefender Manual Scan

If you want to quickly scan a certain folder, you can use the BitDefender Manual Scan.

To access the BitDefender Manual Scan, use the Windows Start menu, by following the path Start \rightarrow Programs \rightarrow BitDefender 2009 \rightarrow BitDefender Manual Scan The following window will appear:



All you have to do is browse the folders, select the folder you want to be scanned and click **OK**. The **BitDefender Scanner** will appear and guide you through the scanning process.

BitDefender Manual Scan



5.6. Game Mode

The new Game Mode temporarily modifies protection settings so as to minimize their impact on system performance. While in Game Mode, the following settings are applied:

- Minimize processor time & memory consumption
- Postpone automatic updates & scans
- Eliminate all alerts and pop-ups
- Scan only the most important files

While in Game Mode, you can see the letter G over the **6** BitDefender icon.

5.6.1. Using Game Mode

If you want to turn Game Mode on, use one of the following methods:

- Right-click the BitDefender icon in the system tray and select Turn on Game Mode.
- Press Ctrl+Shift+Alt+G (the default hotkey).



Important

Do not forget to turn Game Mode off when you finish. To do this, use the same methods you did when you turned it on.

5.6.2. Changing Game Mode Hotkey

If you want to change the hotkey, follow these steps:

- 1. Click Switch to Advanced View (if you are in Basic View).
- 2. Click Game / Laptop Mode from the left side menu.
- 3. Click the Game Mode tab.
- 4. Click the Advanced Settings button.
- 5. Under the Use HotKey option, set the desired hotkey:
 - Choose the modifier keys you want to use by checking one the following: Control key (Ctrl), Shift key (Shift) or Alternate key (Alt).
 - In the edit field, type the letter corresponding to the regular key you want to use.



For example, if you want to use the <code>Ctrl+Alt+D</code> hotkey, you must check only <code>Ctrl</code> and <code>Alt</code> and type <code>D</code>.



Note

Removing the checkmark next to Use HotKey will disable the hotkey.

5.7. Integration into Web Browsers

BitDefender protects you against phishing attempts when you are surfing the Internet. It scans the accessed web sites and alerts you if there are any phishing threats. A White List of web sites that will not be scanned by BitDefender can be configured.

BitDefender integrates directly through an intuitive and easy-to-use toolbar into the following web browsers:

- Internet Explorer
- Mozilla Firefox

You can easily and efficiently manage antiphishing protection and the White List using the BitDefender Antiphishing toolbar integrated into one of the above web browsers.

The antiphishing toolbar, represented by the **SitDefender icon**, is located on the topside of browser. Click it in order to open the toolbar menu.



Note

If you cannot see the toolbar, open the View menu, point to Toolbars and check BitDefender Toolbar.

🖉 Antivirus software - BitDefender - The future of security now! - Windows Internet Explorer	
COO	P •
File Edit View Favorites Tools Help	
Disable software - BitDefender - The future of secur 🛐 🔹 🔂	🔹 🔂 Page 🔹 🎯 Tools 👻 🎇
Add to White List View White List View White List	'um 🗑 Cart 🔒
Help Al Countries/Regions V Search	Go
Company Defense Center Downloads Solutions Support Partners Bu	uy Now
	~
Antiphishing Toolbar	

Getting Started



The following commands are available on the toolbar menu:

Enable / Disable - enables / disables the BitDefender Antiphishing toolbar.



Note

If you choose to disable the antiphishing toolbar, you will no longer be protected against phishing attempts.

Settings - opens a window where you can specify the antiphishing toolbar's settings.

The following options are available:

- Enable Scanning enables antiphishing scanning.
- Ask before adding to whitelist prompts you before adding a web site to the White List.
- Add to White List adds the current web site to the White List.



Note

Adding a site to the White List means that BitDefender will not scan the site for phishing attempts anymore. We recommend you to add to the White List only sites that you fully trust.

View White List - opens the White List.

You can see the list of all the web sites that are not checked by the BitDefender antiphishing engines.

If you want to remove a site from the White List so that you can be notified about any existing phishing threat on that page, click the **Remove** button next to it.

You can add the sites that you fully trust to the White List, so that they will not be scanned by the antiphishing engines anymore. To add a site to the White List, provide its address in the corresponding field and click **Add**.

- Help opens the help file.
- About opens a window where you can see information about BitDefender and where to look for help in case something unexpected appears.

5.8. Integration into Messenger

BitDefender offers encryption capabilities to protect your confidential documents and your instant messaging conversations through Yahoo Messenger and MSN Messenger.

By default, BitDefender encrypts all your instant messaging chat sessions provided that:



- Your chat partner has a BitDefender version installed that supports IM Encryption and IM Encryption is enabled for the instant messaging application used for chatting.
- You and your chat partner use either Yahoo Messenger or Windows Live (MSN) Messenger.



Important

BitDefender will not encrypt a conversation if a chat partner uses a web-based chat application, such as Meebo, or other chat application that supports Yahoo Messenger or MSN.

You can easily configure instant messaging encryption using the BitDefender toolbar from the chat window.

By right-clicking the BitDefender toolbar you will be provided with the following options:

- Permanently enabling / disabling encryption for a certain chat partner
- Inviting a certain chat partner to use encryption
- Removing a certain chat partner from Parental Control blacklist



Instant Messaging Encryption Options

Just click one of the above mentioned options in order to use it.



6. Dashboard

By clicking the Dashboard tab you will be provided with meaningful product statistics and your registration status together with links to the most important on-demand tasks.

BitDefender Antivirus 2009 - Trial SETTINGS SWITCH TO AC			ADVANCED VIEW	
STATUS: There are 2 pe	nding issues			FIX ALL ISSUES
DASHBOARD	ANTIVIRUS CRITICAL WARNING		VULNERABILITY PROTECTED	NETWORK
				Tasks
				> Full System Scan
CRITICAL WARNING				 Deep Scan
				 Update Now
There are 2 issues that affe Overview	ct your system's security.		FIX ALL ISSUES	
Registration:		Last update:	Never	
Expires in:		Last scan:	Never	
	30 days left	Next scan:	Never	
Q				
(Spitdefender			My Account - Register	- <u>Help</u> - <u>Support</u> - <u>History</u>
Dashboard				

6.1. Overview

This is where you can see a summary of statistics regarding the update status, your account status, registration and license information.

Item	Description
Last update	Indicates the date when your BitDefender product was last updated. Please perform regular updates in order to have a fully protected system.
My account	Indicates the e-mail address that you can use to access your on-line account to recover your lost BitDefender license key



ltem	Description
	and to benefit from BitDefender support and other customized services.
Registration	Indicates your license key type and status. To keep your system safe you must renew or upgrade BitDefender if your key has expired.
Expires in	Indicates the number of days left until the license key expires.

To update BitDefender just click the Update Now button from the tasks section.

To create or to login to your BitDefender account, follow these steps.

- 1. Click the **My Account** link from the bottom of the window. A web page will open.
- 2. Type your username and password and click the **Login** button.
- 3. To create a BitDefender account, select **You don't have an account?** and provide the required information.



Note

The data you provide here will remain confidential.

To register BitDefender Antivirus 2009, follow these steps.

- 1. Click the **My Account** link from the bottom of the window. A one-step registration wizard will open.
- 2. Click the I want to register the product with a new key radio button.
- 3. Type the new license key in the corresponding textbox.
- 4. Click Finish.

To buy a new license key, follow these steps.

- 1. Click the **My Account** link from the bottom of the window. A one-step registration wizard will open.
- 2. Click the Renew Your BitDefender License Key link. A web page will open.
- 3. Click the **Buy Now** button.

6.2. Tasks

This is where you can find links to the most important security tasks: full system scan, deep scan, update now.



The following buttons are available:

- Full System Scan starts a full scan of your computer (archives excluded).
- **Deep Scan** starts a full scan of your computer (archives included).
- Update Now starts an immediate update.

6.2.1. Scanning with BitDefender

To scan your computer for malware, run a particular scan task by clicking the corresponding button. The following table presents the available scan tasks, along with their description:

Task	Description
Full System Scan	Scans the entire system, except for archives. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.
Deep Scan	Scans the entire system. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.



Note

Since the **Deep System Scan** and **Full System Scan** tasks analyze the entire system, the scanning may take a while. Therefore, we recommend you to run these tasks on low priority or, better, when your system is idle.

When you initiate an on-demand scanning process, whether a quick or a full scan, the BitDefender Scanner will appear.

Follow the three-step guided procedure to complete the scanning process.

6.2.2. Updating BitDefender

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 checks for updates when you turn on your computer and **every hour** after that. However, if you want to update BitDefender, just click **Update Now**. The update process will be initiated and the following window will appear immediately:



Bit Defender Antivi	rus 2009		_ X
Update			
	S	tep 1	
BitDefender Update			
BitDefender will perform the task process will finish, an On-deman	selected during the previous step. Belo d scan will start.	w you can check the status for the Upda	te process. As soon as the update
Status: Checking for	updates		
File:	0%	0 kb	
Total Update:	28 %	0 kb	
Q			
(Spitdefender)			Finish Cancel
Updating BitDefer	ıder		

In this window you can see the status of the update process.

The update process is performed on the fly, meaning that the files to be updated are replaced progressively. In this way, the update process will not affect product operation and, at the same time, all vulnerabilities will be excluded.

If you want to close this window, just click **Cancel**. However, this will not stop the update process.



Note

If you are connected to the Internet through a dial-up connection, then it is recommended to regularly update BitDefender by user request.

Restart the computer if required. In case of a major update, you will be asked to restart your computer.

Click **Reboot** to immediately reboot your system.

If you want to reboot your system later, just click **OK**. We recommend that you reboot your system as soon as possible.



7. Antivirus

BitDefender comes with an Antivirus module that helps you keep your BitDefender up to date and your computer virus free.

BitDefender Antivirus 2009 - Trial		SETTINGS SWITCH TO		
STATUS: There are 2 pe	nding issues			FIX ALL ISSUES
DASHBOARD	ANTIVIRUS CRITICAL WARNING	ANTIPHISHING PROTECTED	VULNERABILITY PROTECTED	NETWORK
Monitored Compone	nts		Expand/Collapse All	Tasks
 Local security 		Monitor	Status 🔺	→ Full System Scan
Real time file protection is e	nabled	✓ Yes	ОК	→ Deep Scan
You have never scanned	l your computer for malware	🖌 Yes	Fix	My Documents Scan
The update has never b	een performed	✓ Yes	Fix	 Update Now
				→ Scan Wizard
			V	
Q				
(Spitdefender)			My Account - Register	- <u>Help</u> - <u>Support</u> - <u>History</u>
Antivirus				

To enter the Antivirus module, click the Antivirus tab.

The Antivirus module consists of two sections:

- Monitored Components Allows you to see the full list of monitored components for each security module. You can choose which of the modules to be monitored. It is recommended to enable monitoring all components.
- **Tasks** This is where you can find links to the most important security tasks: full system scan, deep scan, update now.

7.1. Monitored Components

The monitored component is the following:



Category	Description
Local security	This is where you can check the status of each security modules that protects objects stored on your computer (files, registry, memory, etc).

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

7.1.1. Local security

We know it's important to be noticed whenever a problem can affect your computer's security. By monitoring each security modules, BitDefender Antivirus 2009 will let you know not only when you configure the settings that might affect your computer's security, but when you forget to do important tasks.

The issues concerning local security are described in very explicit sentences. In line with each sentence, if there is something that might affect your computer's security, you will see a red status button called **Fix**. Otherwise, a green **OK** status button is displayed.

Issue	Description
Real time file protection is enabled	Ensures that all files are scanned as they are accessed by you or by an application running on this system.
You have scanned your computer for malware today	It is highly recommended to run an on demand scan as soon as possible to check if files stored on your computer are malware free.
Automatic update is enabled	Please keep automatic update enabled to ensure that the malware signatures of your BitDefender product are updated on a regular basis.
Updating now	Product and malware signatures update is being performed.

When the status buttons are green, the security risk of your system is at a minimum. To turn the buttons green, follow these steps:

- 1. Click the Fix buttons to fix security vulnerabilities one by one.
- 2. If one issue is not fixed on the spot, follow the wizard to fix it.



If you want to exclude an issue from monitoring, just clear the **Yes, monitor this component** checkbox.

7.2. Tasks

This is where you can find links to the most important security tasks: full system scan, deep scan, update now.

The following buttons are available:

- Full System Scan starts a full scan of your computer (archives excluded).
- Deep Scan starts a full scan of your computer (archives included).
- Scan My Documents starts a quick scan of your documents and settings.
- Update Now starts an immediate update.
- Custom scan

7.2.1. Scanning with BitDefender

To scan your computer for malware, run a particular scan task by clicking the corresponding button. The following table presents the available scan tasks, along with their description:

Task	Description
Full System Scan	Scans the entire system, except for archives. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.
Deep Scan	Scans the entire system. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.
Scan My Documents	Use this task to scan important current user folders: My Documents, Desktop and StartUp. This will ensure the safety of your documents, a safe workspace and clean applications running at startup.
Custom scan	Use this task to choose specific files and folders to be scanned.



1

Note

Since the **Deep System Scan** and **Full System Scan** tasks analyze the entire system, the scanning may take a while. Therefore, we recommend you to run these tasks on low priority or, better, when your system is idle.

When you initiate an on-demand scanning process, whether a quick or a full scan, the BitDefender Scanner will appear.

Follow the three-step guided procedure to complete the scanning process.

Custom scan

By clicking the **Custom scan** button and following the wizard, you can create custom scan tasks and optionally save them as quick tasks.

Step 1/4 - Welcome Window

 BitDefender 2009
 Image: The Step 1 of 4

 Secon Wizard - Step 1 of 4
 Step 2
 Step 3
 Step 4

 Welcome
 This Weard will help you scen your computer for any threat that might affect it. You will be able to select specific folders and/or files to be scanned as well as define the actions to be taken on infected files. You will also environ that will help you assess the security level of your system.

 Image: Step the step in future scans
 Skep this step in future scans

 Image: Step the step of this weard to configure the scanning process according to your needs.
 Image: Step the step of this weard to configure the scanning process according to your needs.

 Image: Step the step of this weard to configure the scanning process according to your needs.
 Image: Step the step of this weard to configure the scanning process according to your needs.

 Image: Step the step of this weard to configure the scanning process according to your needs.
 Image: Step the step of this weard to configure the scanning process according to your needs.

 Image: Step the step of this weard to configure the scanning process according to your needs.
 Image: Step the step of this weard to configure the scanning process according to your needs.

 Image: Step the step of this weard to configure the scanning process according to your needs.
 Image: Step the step of this weard to configure the scanning process according to your needs.

 Image: Step the step of this weard to configure the scanning process according to your needs.
 Image: Step the step the step the s

This is just a welcome page.



This wizard will help you scan your computer for any threat that might affect it. You will be able to select specific folders and/or files to be scanned as well as define the actions to be taken on infected files. You will also receive a scan report that will help you assess the security level of your system. Please go through each step and configure the scanning process according to your needs.



Note

To skip this step in future scans just select the corresponding checkbox.

Click Next to continue or click Cancel if you want to quit the wizard.

Step 2/4 - Select Items to be Scanned

In this step, you can choose the files and folders to be scanned.



Click Browse to select specific folders and/or files from your computer. The following options are available:

Option	Description		
Scan all selected items	Select this option to scan only the items selected before.		
Scan program files only	Select this option to scan only programs and applications.		
Scan only user defined extensions	Select this option to scan only the specific extensions that you would like to be scanned. A new textbox will appear where you can type them.		
	Note Extensions must be separated by a semicolon (e.g.: exe;com;ivd;)		

Click Next to continue or click Cancel if you want to quit the wizard.

Step 3/4 - Select the Actions to be Taken

In this step, you can choose what actions should be taken against the found threats and you can select a scanning options by using the slider.



BitDefender 2009			_ ×
Scan Wizard - Step 3 of 4			
Step	l Step2	Step3	Step
Action Options			
When an infected file is found		Disinfe	ect it 💽
When an suspect file is found		Take r	io action 💽 💌
When an hidden file is found		Take r	no action 💽
Scan level			
- High	Medium level		
🗈 Medium	- default, moderate resource consumption		
· Low	- scan for viruses and spyware		
- Custom			
In this step, you can choose what	actions should be taken against the found threats and you can sele	ct a scanning options by using the slider.	
(Spitdefender)		6	ancel Back Next
Select the Actions	to be Taken		

You can select from the corresponding menu the action to be taken:

- When an infected file is found
- When a suspicious file is found
- When a hidden file is found

At the same time, you can configure the protection level of the scanning. 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 4 protection levels:

Protection level	Description
High	Offers high security. The resource consumption level is high.
	 scan all files and archives scan for viruses and spyware



Protection level	Description
	scan for hidden files and proceses
Medium	Offers medium security. The resource consumption level is moderate. scan all files scan for viruses and spyware
Low	Covers basic security needs. The resource consumption level is very low. scan programs files only scan for viruses
Custom	This is where you can select your own scanning options. Click Customize and set the scan level. Select the check-box(es) for each type of malware you want to be searched on your computer during the scanning process.

Click Next to continue or click Cancel if you want to quit the wizard.

Step 4/4 - Set Additional Options

In this step, you can set additional options before starting the scanning.



BitDefender 2009			_ ×
Scan Wizard - Step 4 of 4			
Step 1	Step2	Step3	Step4
Aditional Options			
Save this as a quick task			
Quick task name			
Shut down the computer after scan if no the	reats are found		
Save the current scanning process as a scanning task in o	rder to be able to use it as such in the futu	re,	
(bit defender		Cancel	Back Start Scan

Set Additional Options

To save the scanning task in order to use it as such in the future, select the corresponding checkbox and type a convenient name into the textbox.



Note

A new button with the above mentioned name will appear under the tasks menu.

If you want to shut down the computer after scanning select the corresponding checkbox.

Click **Start Scan** and follow the three-step guided procedure to complete the scanning process.

7.2.2. Updating BitDefender

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 checks for updates when you turn on your computer and **every hour** after that. However, if you want to update BitDefender, just click **Update Now**. The update process will be initiated and the following window will appear immediately:

Bit Defender Antivirus 2009 -			
Update			
	Step 1		
BitDefender Update			
BitDefender will perform the task selected d process will finish, an On-demand scan will s	uring the previous step. Below you can check the statu tart.	s for the Update pr	ocess. As soon as the update
Status: Checking for updates			
File:	0 %	0 kb	
Total Update:	28 %	0 kb	
Q			
Spitdefender			Finish Cancel
Updating BitDefender			

In this window you can see the status of the update process.

The update process is performed on the fly, meaning that the files to be updated are replaced progressively. In this way, the update process will not affect product operation and, at the same time, all vulnerabilities will be excluded.

If you want to close this window, just click **Cancel**. However, this will not stop the update process.



Note

If you are connected to the Internet through a dial-up connection, then it is recommended to regularly update BitDefender by user request.

Restart the computer if required. In case of a major update, you will be asked to restart your computer.



Click Reboot to immediately reboot your system.

If you want to reboot your system later, just click **OK**. We recommend that you reboot your system as soon as possible.



8. Antiphishing

BitDefender comes with an Antiphishing module that ensures that all web pages access by you via Internet Explorer or Firefox are safe.

To enter the Antiphishing module, click the Antiphishing tab.

BitDefender Antivirus 2009 - Trial SETTINGS SWITCH TO ADVANCED VIEW		ADVANCED VIEW	
STATUS: There are 2 pending issues			FIX ALL ISSUES
DASHBOARD ANTIVIRUS CRITICAL WARNING	ANTIPHISHING PROTECTED	VULNERABILITY PROTECTED	NETWORK
Monitored Components		Expand/Collapse All	Tasks
Online security		OK 🔺	> Full System Scan
			→ Deep Scan
			 Update Now
0		v	
C.			
(Spitdefender		My Account - Register -	- <u>Help</u> - <u>Support</u> - <u>History</u>
Antiphishing			

The Antiphishing module consists of two sections:

- Monitored Components Allows you to see the full list of monitored components for each security module. You can choose which of the modules to be monitored. It is recommended to enable monitoring all components.
- **Tasks** This is where you can find links to the most important security tasks: full system scan, deep scan, update now.

8.1. Monitored Components

The monitored component is the following:



Category	Description
Online security	This is where you can check the status of each security modules that protects your online transactions and your computer while connected to internet.

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

8.1.1. Online security

The issues concerning online security are described in very explicit sentences. In line with each sentence, if there is something that might affect your computer's security, you will see a red status button called **Fix**. Otherwise, a green **OK** status button is displayed.

Issue	Description
Conversation encryption for IM is enabled	If your IM contacts have BitDefender 2009 installed, all IM discussions via Yahoo! Messenger and Windows Live Messenger will be encrypted. It is recommended to have conversation encryption for IM enabled to ensure that your IM conversations remain private.
Firefox antiphishing protection is enabled	BitDefender protects you against phishing attempts when you are surfing the Internet.
Internet Explorer antiphishing protection is enabled	BitDefender protects you against phishing attempts when you are surfing the Internet.

When the status buttons are green, the security risk of your system is at a minimum. To turn the buttons green, follow these steps:

- 1. Click the **Fix** buttons to fix security vulnerabilities one by one.
- 2. If one issue is not fixed on the spot, follow the wizard to fix it.

If you want to exclude an issue from monitoring, just clear the **Yes, monitor this component** checkbox.



8.2. Tasks

This is where you can find links to the most important security tasks: full system scan, deep scan, update now.

The following buttons are available:

- Full System Scan starts a full scan of your computer (archives excluded).
- Deep Scan starts a full scan of your computer (archives included).
- Scan My Documents starts a quick scan of your documents and settings.
- **Update Now** starts an immediate update.
- Custom scan

8.2.1. Scanning with BitDefender

To scan your computer for malware, run a particular scan task by clicking the corresponding button. The following table presents the available scan tasks, along with their description:

Task	Description
Full System Scan	Scans the entire system, except for archives. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.
Deep Scan	Scans the entire system. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.
Scan My Documents	Use this task to scan important current user folders: ${\tt My}$ ${\tt Documents}, {\tt Desktop}$ and ${\tt StartUp}.$ This will ensure the safety of your documents, a safe workspace and clean applications running at startup.
Custom scan	Use this task to choose specific files and folders to be scanned.



Note

Since the **Deep System Scan** and **Full System Scan** tasks analyze the entire system, the scanning may take a while. Therefore, we recommend you to run these tasks on low priority or, better, when your system is idle.



When you initiate an on-demand scanning process, whether a quick or a full scan, the BitDefender Scanner will appear.

Follow the three-step guided procedure to complete the scanning process.

Custom scan

By clicking the **Custom scan** button and following the wizard, you can create custom scan tasks and optionally save them as quick tasks.

Step 1/4 - Welcome Window

This is just a welcome page.

BitDefender 2009			_ ×
Scan Wizard - Step 1 of 4			
Step 1	Step2	Step3	Step4
Welcome			
This wizard will help you scan your computer for any th well as define the actions to be taken on infected files. Please go through each step and configure the scannin	reat that might affect it. You will be ab You will also receive a scan report that g process according to your needs.	le to select specific folders and/or files : will help you assess the security level	to be scanned as of your system.
Skip this step in future scans			
Go through each step of this wizard to configure the scar	ning process according to your needs.		
Stidefender			Cancel Next
Welcome Window			

This wizard will help you scan your computer for any threat that might affect it. You will be able to select specific folders and/or files to be scanned as well as define the actions to be taken on infected files. You will also receive a scan report that will help you assess the security level of your system. Please go through each step and configure the scanning process according to your needs.





To skip this step in future scans just select the corresponding checkbox.

Click Next to continue or click Cancel if you want to quit the wizard.

Step 2/4 - Select Items to be Scanned

Note

In this step, you can choose the files and folders to be scanned.

BitDefender 2009			_ ×
Scan Wizard - Step 2 of 4			
Step 1	Step2	Step3	Step4
Scanned Items			
Choose the files and folders to be scanned.			
Browse			
Scan all selected items			
Scan program files only			
Scan only user defined extensions			
-			
In this step, you can choose the files and folders to be scanne	d.		
(Spitdefender			Cancel Next
Select Items to be Scanned			

Click Browse to select specific folders and/or files from your computer. The following options are available:

Option	Description
Scan all selected items	Select this option to scan only the items selected before.
Scan program files only	Select this option to scan only programs and applications.



Option	Description	
Scan only user defined extensions	Select this option to scan only the specific extensions that you would like to be scanned. A new textbox will appear where you can type them.	
	Note Extensions must be separated by a semicolon (e.g.: exe;com;ivd;)	

Click Next to continue or click Cancel if you want to quit the wizard.

Step 3/4 - Select the Actions to be Taken

In this step, you can choose what actions should be taken against the found threats and you can select a scanning options by using the slider.

BitDefender 2009			_ ×
Scan Wizard - Step 3 of 4			
Step 1	Step2	Step3	Step4
Action Options			
When an infected file is found		Disinfect it	•
When an suspect file is found		Take no act	ion 💌
When an hidden file is found		Take no act	ion 💽
Scan level			
- High	Medium level		
 Medium Low Custom 	 default, moderate resource consumption scan all files scan for viruses and spyware 		
In this step, you can choose what a	ctions should be taken against the found threats and you can sel	lect a scanning options by using the slider.	Rack Nevt
Select the Actions t	o be Taken	Conte	Duck Next

You can select from the corresponding menu the action to be taken:



- When an infected file is found
- When a suspicious file is found
- When a hidden file is found

At the same time, you can configure the protection level of the scanning. 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 4 protection levels:

Protection level	Description
High	 Offers high security. The resource consumption level is high. scan all files and archives scan for viruses and spyware scan for hidden files and proceses
Medium	Offers medium security. The resource consumption level is moderate. scan all files scan for viruses and spyware
Low	Covers basic security needs. The resource consumption level is very low. scan programs files only scan for viruses
Custom	This is where you can select your own scanning options. Click Customize and set the scan level. Select the check-box(es) for each type of malware you want to be searched on your computer during the scanning process.

Click Next to continue or click Cancel if you want to quit the wizard.

Step 4/4 - Set Additional Options

In this step, you can set additional options before starting the scanning.


BitDefender 2009			_ ×
Scan Wizard - Step 4 of 4			
Step1	Step2	Step3	Step4
Aditional Options			
Save this as a quick task			
Quick task name			
Shut down the computer after scan if no thr	eats are found		
${igodot}$ Save the current scanning process as a scanning task in or	der to be able to use it as such in the fut	ure.	
Stidefender		Cancel B	ack Start Scan
Set Additional Options			

•

To save the scanning task in order to use it as such in the future, select the corresponding checkbox and type a convenient name into the textbox.



Note

A new button with the above mentioned name will appear under the tasks menu.

If you want to shut down the computer after scanning select the corresponding checkbox.

Click **Start Scan** and follow the three-step guided procedure to complete the scanning process.

8.2.2. Updating BitDefender

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 checks for updates when you turn on your computer and **every hour** after that. However, if you want to update BitDefender, just click **Update Now**. The update process will be initiated and the following window will appear immediately:

Bit Defender Antivirus 200	9		_ ×
Update			
	Step 1		
BitDefender Update			
BitDefender will perform the task selected du process will finish, an On-demand scan will st	ring the previous step. Below you can check the status art.	; for the Upda	te process. As soon as the update
Status: Checking for updates			
File:	0 %	0 kb	
Total Update:	28 %	0 kb	
Q			
Stidefender			Finish Cancel
Updating BitDefender			

In this window you can see the status of the update process.

The update process is performed on the fly, meaning that the files to be updated are replaced progressively. In this way, the update process will not affect product operation and, at the same time, all vulnerabilities will be excluded.

If you want to close this window, just click **Cancel**. However, this will not stop the update process.



Note

If you are connected to the Internet through a dial-up connection, then it is recommended to regularly update BitDefender by user request.

Restart the computer if required. In case of a major update, you will be asked to restart your computer.



Click Reboot to immediately reboot your system.

If you want to reboot your system later, just click **OK**. We recommend that you reboot your system as soon as possible.



9. Vulnerability

BitDefender comes with a Vulnerability module that helps you keep crucial software on your PC up-to-date.

To enter the Vulnerability module, click the Vulnerability tab.

BitDefender Antiv	irus 2009 - Trial		SETTINGS SWITCH TO	ADVANCED VIEW
STATUS: There are 2 pe	ending issues			FIX ALL ISSUES
DASHBOARD	ANTIVIRUS CRITICAL WARNING	ANTIPHISHING PROTECTED	VULNERABILITY REQUIRES ATTENTION	NETWORK
Monitored Compone	nts		Expand/Collapse All	Tasks
 ¥ulnerability scan 		Monitor	Status 🔺	→ ¥ulnerability Scan
Vulnerability check is enab	led	No No	Not monitored	
Critical Microsoft updates		No No	Not monitored	
Other Microsoft updates		No No	Not monitored	
Windows Automatic Upda	tes is enabled	✔ Yes	ОК	
Firefox (Out Of Date)		✔ Yes	More Info	
Administrator (Strong Pas	sword)	✔ Yes	ОК	
test (Weak Password)		No	Not monitored	
			Ţ	
Q				
(Spitdefender)			My Account - Register	- <u>Help</u> - <u>Support</u> - <u>History</u>
Vulnerability				

The Vulnerability module consists of two sections:

- Monitored Components Allows you to see the full list of monitored components for each security module. You can choose which of the modules to be monitored. It is recommended to enable monitoring all components.
- **Tasks** This is where you can find link to one of the most important security task.

9.1. Monitored Components

The monitored component is the following:



Category	Description
Vulnerability scan	This is where you can check whether crucial software on your PC is up-to-date. Passwords to Windows accounts are checked against security rules.

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

9.1.1. Vulnerability scan

The issues concerning vulnerabilities are described in very explicit sentences. In line with each sentence, if there is something that might affect your computer's security, you will see a red status button called **Fix**. Otherwise, a green **OK** status button is displayed.

Issue	Description
Vulnerability check is enabled	Monitors Microsoft Windows Updates, Microsoft Windows Office Updates and Microsoft Windows accounts passwords to ensure that your OS is up to date and is not vulnerable to password bypass.
Critical Microsoft updates	Install available critical Microsoft updates.
Other Microsoft updates	Install available non-critical Microsoft updates.
Windows Automatic Updates is enabled	Install new Windows security updates as soon as they become available.
Admin (Strong Password)	Indicates the password's strength for specific users.

When the status buttons are green, the security risk of your system is at a minimum. To turn the buttons green, follow these steps:

- 1. Click the **Fix** buttons to fix security vulnerabilities one by one.
- 2. If one issue is not fixed on the spot, follow the wizard to fix it.

If you want to exclude an issue from monitoring, just clear the **Yes, monitor this component** checkbox.



9.2. Tasks

This is where you can find link to one of the most important security tasks.

The following button is available:

Vulnerability Scan

9.2.1. Searching for Vulnerabilities

Vulnerability Scan checks Microsoft Windows Updates, Microsoft Windows Office Updates and the passwords to your Microsoft Windows accounts to ensure that your OS is up to date and that it is not vulnerable to password bypass.

To check your computer for vulnerabilities, click $\ensuremath{\textbf{Vulnerability Scan}}$ and follow the wizard.



Step 1/6 - Select Vulnerabilities to Check

Bit Defender Ar	ntivirus 2009				_ ×
Vulnerability Scan					
Step 1 - Select tasks	Step 2 - Scanning	Step 3 - Passwords	Step 4 - Applications	Step 5 - Windows	Step 6 - Finish
Select tasks					
The wizard searches for av- applications that are checke select all the boxes below.	ailable Windows updates, v d for these vulnerabilities.	weak passwords to Win . In order for all of thes	dows accounts and outdated e applications to be fully upo	d applications. BitDefender o lated and protected, it is rec	ontains a list of ommended to
 User Passwords 					
Applications Updates					
Critical Windows Update	ates				
Other Windows Upda	tes				
Select the actions th	e vulnerability module sho	uld take when checking	your system.		
Contaciender					Next Cancel
/ulnerabilities					

Click Next to check the system for the selected vulnerabilities.



Step 2/6 - Checking for Vulnerabilities

Bit Defender Ar	ntivirus 2009				_ ×
Vulnerability Scan					
Step 1 - Select tasks	Step 2 - Scanning	Step 3 - Passwords	Step 4 - Applications	Step 5 - Windows	Step 6 - Finish
Status					
Scanning	🐛 Critical Windows	Updates			
C The scanning proces	s is in progress				
(Spitdefender)					Stop Cancel
Vulnerability C	heck				

Wait for BitDefender to finish checking for vulnerabilities.



Step 3/6 - Change Weak Passwords

unerability Scari					
Step 1 - Select tasks	Step 2 - Scanning	Step 3 - Passwords	Step 4 - Applications	Step 5 - Windows	Step 6 - Fini
ser Passwords					
Jser Name	Streng	th Status			
Administrator	Strong	Ok			
cosmin	Weak	Fix			
This is a list of the U	vindows accounts passwor s.	ds set on your computer a	nd the level of protection t	hat they provide. Click the 'I	=ix' button to mo
the weak passwords					

You can see the list of the Windows user accounts configured on your computer and the level of protection their password provides.

Click Fix to modify the weak passwords. A new window will appear.

BitDefender
Choose method to fix:
 Force user to change password at next login Change user password
Type password:
Confirm password:
OK Clase
Change Password



Select the method to fix this issue:

- Force user to change password at next login. BitDefender will prompt the user to change the password the next time the user logs on to Windows.
- **Change user password.** You must type the new password in the edit fields.



Note

For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, \$ or @).

Click **OK** to change the password.

Click Next.

Step 4/6 - Update Applications

Bit Defender Ant	tivirus 2009				-	_ ×
Vulnerability Scan						
Step 1 - Select tasks	Step 2 - Scanning	Step 3 - Passwords	Step 4 - Applications	Step 5 - Windows	Step 6	- Finish
Applications Updates						
Application Name		I	nstalled Version	Latest Version	Download	
Yahoo! Messenger			8.1.0.421	8.1.0.241	Up To Date	
Winamp			5,5,3,1938	5,5,3,1924	Up To Date	
Firefox			2.0.0.15 (en-US)	3.0 (en-US)	Home Page	
						Y
C This is a list of the app	lications supported by B	itDefender and of the up	dates available, if any.			
(<i>bitdefender</i>)					Next C	ancel
Applications						

You can see the list of applications checked by BitDefender and if they are up to date. If an application is not up to date, click the provided link to download the latest version.



Click Next.

Step 5/6 - Update Windows

					/ulnerability Scan
Step 6 - Finis	Step 5 - Windows	Step 4 - Applications	Step 3 - Passwords	Step 2 - Scanning	Step 1 - Select tasks
					Windows Updates
				ates	Critical Windows Upd
		31)	Service Pack 2 (KB93618	oft XML Core Services 4.0	Security Update for Microso
				tes	Other Windows Upda
				category	No updates available in this
				tes	Tnstall All System Upda
			pplications updates	tes	Install All System Upda

You can see the list of critical and non-critical Windows updates that are not currently installed on your computer. Click **Install All System Updates** to install all the available updates.

Click Next.



Step 6/6 - View Results

<mark>it</mark> Defender Ant	tivirus 2009				_ ×
ulnerability Scan					
Step 1 - Select tasks	Step 2 - Scanning	Step 3 - Passwords	Step 4 - Applications	Step 5 - Windows	Step 6 - Finisl
The vulnerability	scan is finished. 1	The tasks you selec	ted at Step 1 have l	een performed.	
The vulnerability scan	is finished. The tasks y	ou selected at Step 1 have	e been performed.		

Click Close.



10. Network

The Network module allows you to manage the BitDefender products installed on your home computers from a single computer.

BitDefender Antiv	irus 2009 - Trial		SETTINGS SWITCH TO	ADVANCED VIEW
STATUS: There is 1 pen	ding issue			FIX ALL ISSUES
DASHBOARD		ANTIPHISHING PROTECTED	VULNERABILITY PROTECTED	NETWORK Tasks Join/Create Network
empty empty empty		empty empty empty		
Q (Sbitdefender			<u>My Account</u> - <u>Register</u>	- <u>Help</u> - <u>Support</u> - <u>History</u>
Network				

To enter the Network module, click the File Manager tab.

To be able to manage the BitDefender products installed on your home computers, you must follow these steps:

- 1. Join the BitDefender home network on your computer. Joining the network consists in configuring an administrative password for the home network management.
- 2. Go to each computer you want to manage and join the network (set the password).
- 3. Go back to your computer and add the computers you want to manage.

10.1. Tasks

Initially, one button is available only.



Join/Create Network - allows you to set the network password, thus entering the network.

After joining the network, several more buttons will appear.

- Leave Network allows you to leave the network.
- Manage Network allows you to add computer to your network.
- **Scan All** allows you to scan all managed computers at the same time.
- **Update All** allows you to update all managed computers at the same time.
- **Register All** allows you to register all managed computers at the same time.

10.1.1. Joining the BitDefender Network

To join the BitDefender home network, follow these steps:

1. Click **Join/Create network**. You will be prompted to configure the home management password.

BitDefender		×
Enter the home manage	ement password	
The password should be at	least 8 characters long	
Enter password:	•••••	
Retype password:	•••••	
ок	Cancel	

Configure Password

- 2. Type the same password in each of the edit fields.
- 3. Click OK.

You can see the computer name appearing in the network map.

10.1.2. Adding Computers to the BitDefender Network

Before you can add a computer to the BitDefender home network, you must configure the BitDefender home management password on the respective computer.

To add a computer to the BitDefender home network, follow these steps:



1. Click **Manage Network**. You will be prompted to provide the local home management password.

Bit Defender	
You must enter the home management password.	
Password:	••••••
Don't show thi	s message again this session.
	OK Cancel
Enter Passv	vord

2. Type the home management password and click **OK**. A new window will appear.

BitDefender ×
Computer
scohen
scripts2
sdediu
sgheorghe
sgheorghe2
sorel 🔤
🛒 sqib01 🗸
IP (or hostname) 10.10.13.59
Please select the computers that you want to add to your network.
Add Cancel
Add Computer

You can see the list of computers in the network. The icon meaning is as follows:

- 🗐 Indicates an online computer with no BitDefender products installed.
- Indicates an online computer with BitDefender installed.



- Indicates an offline computer with BitDefender installed.
- 3. Do one of the following:
 - Select from the list the name of the computer to add.
 - Type the IP address or the name of the computer to add in the corresponding field.
- 4. Click **Add**. You will be prompted to enter the home management password of the respective computer.

BitDefender	×
Enter Remote HM Password	
The password should be at least 8 characters long	
Enter Remote Password	
OK Cancel	
Authenticate	

- 5. Type the home management password configured on the respective computer.
- 6. Click **OK**. If you have provided the correct password, the selected computer name will appear in the network map.



Note

You can add up to five computers to the network map.

10.1.3. Managing the BitDefender Network

Once you have successfully created a BitDefender home network, you can manage all BitDefender products from a single computer.

BitDefender Antivirus 2009 - Trial			SETTINGS SV	ИТСН ТО	ADVANCED VIEW
STATUS: There is 1	pending issue				FIX ALL ISSUES
DASHBOARD	ANTIVIRUS CRITICAL WARNING	ANTIPHISHING PROTECTED	VULNERAE PROTECT	BILITY	NETWORK
	NTERNET		RDENTI 405-YD		Tasks
			10.10.15.29 1 issues Trial		> Leave Network
(No gateway four	nd!			 Add Computer
			10		→ Scan All
This Comput	BLENTLAPS-7 This Comput Set the settings password. No PC (click t No PC (click t		ck to add)		→ Update All
No PC (dick t			du to add)		 Register All
	Fix issues on this computer Show bistory of this computer	CK to a			
No PC (dick t	Run an Update on this computer n Apply Profile	iow , ck to a	dd)		
	Set this computer as Update Serve	er of this Network		¥	
Q					
(Spitdefender)			My Account	- <u>Register</u>	- <u>Help</u> - <u>Support</u> - <u>History</u>
Network Map					

If you move the mouse cursor over a computer from the network map, you can see brief information about it (name, IP address, number of issues affecting the system security, BitDefender registration status).

If you right-click a computer name in the network map, you can see all the administrative tasks you can run on the remote computer.

- Register this computer
- Set the settings password
- Run a scan task
- Fix issues on this computer
- Show history of this computer
- Run an update on this computer now
- Apply profile
- Run a Tuneup task on this computer
- Set this computer as Update Server of this Network



Before running a task on a specific computer, you will be prompted to provide the local home management password.

Bit Defende	r	
You must ent	er the home management password.	
Password:	•••••	
Don't show	this message again this session.	
	OK Cancel	
Enter Pass	word	

Type the home management password and click OK.



Note

If you plan to run several tasks, you might want to select **Don't show this message again this session**. By selecting this option, you will not be prompted again for this password during the current session.

10.1.4. Scanning All Computers

To scan all managed computers, follow these steps:

1. Click **Scan All**. You will be prompted to provide the local home management password.

Defender	
You must enter	the home management password.
Password:	•••••
Don't show thi	is message again this session.
	OK Canad



- 2. Select a scan type.
 - Full System Scan starts a full scan of your computer (archives excluded).
 - Deep Scan starts a full scan of your computer (archives included).
 - **Scan My Documents** starts a quick scan of your documents and settings.



3. Click OK.

10.1.5. Updating All Computers

To update all managed computers, follow these steps:

1. Click **Update All**. You will be prompted to provide the local home management password.



Linter Fassword

2. Click OK.



10.1.6. Registering All Computers

To register all managed computers, follow these steps:

1. Click **Register All**. You will be prompted to provide the local home management password.

it Defender	
You must enter	the home management password.
Password:	•••••
Don't show th	is message again this session.
	OK Cancel

2. Enter the key you want to register with.



- Register All
- 3. Click OK.



11. Basic Settings

The Basic Settings module is the place where you can easily enable or disable important security modules.

To enter the Basic Settings module, click the **Settings** button from the upper part of the Basic View.

Local security	Status	
Real-Time Antivirus & Antispyware File Protection	🖌 Enabled	
Automatic Update	🖌 Enabled	
Automatic Vulnerability Check	🖌 Enabled	
Online security	Status	
Real-Time Antivirus, Antispam & Antiphishing Mail Protection	🖌 Enabled	
Real-Time Antivirus & Antispyware Web Protection	Disabled	
Real-Time Antiphishing Web Protection	🖌 Enabled	
Identity Control	🖌 Enabled	
IM Encryption	🖌 Enabled	
General settings	Status	
Game Mode	Disabled	
Laptop Mode Detection	🖌 Enabled	
0		
		cl
		LIOS

The available security modules have been grouped into several categories.

Category	Description
Local security	This is where you can enable / disable real time file protection or the automatic update.
Online security	This is where you can enable / disable real time mail and web protection.
General settings	This is where you can enable / disable game mode, laptop mode, passwords, scan activity bar and more.

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



11.1. Local security

You can enable / disable security modules with one click.

Security module	Description
Real-Time Antivirus & Antispyware File Protection	Real-time file protection ensures that all files are scanned as they are accessed by you or by an application running on this system.
Automatic Update	Automatic update ensures that the newest BitDefender product and signature files are downloaded and installed automatically on a regular base.
Automatic Vulnerability Check	Automatic vulnerability check ensures that crucial software on your PC are up-to-date.

11.2. Online security

You can enable / disable security modules with one click.

Security module	Description
Real-Time Antiphishing Web Protection	Real-time web antiphishing protection ensures that all files downloaded via HTTP are scanned for phishing attempts.
Identity control	Identity Control helps you keep confidential data safe by scanning all web and mail traffic for specific strings.
IM Encryption	If your IM contacts have BitDefender 2009 installed, all IM conversations via Yahoo! Messenger and Windows Live Messenger will be encrypted.

11.3. General settings

You can enable / disable security related items with one click.

ltem	Description
Game Mode	Game Mode temporarily modifies protection settings so as to
	minimize their impact on system performance during games.



ltem	Description
Laptop Mode	Laptop Mode temporarily modifies protection settings so as to minimize their impact on the life of your laptop battery.
Settings Password	This ensures that the BitDefender settings can only be changed by the person who knows this password.
BitDefender News	By enabling this option, you will receive important company news, product updates or new security threats from BitDefender.
Products Notification Alerts	By enabling this option, you will receive information alerts.
Scan Activity Bar	The Scan Activity Bar is a small, transparent bar indicating the progress of the BitDefender scanning activity. The green flowing line shows the scanning activity on your local system. The red flowing line shows the scanning activity on your internet connection.
Load BitDefender at Startup	By enabling this option, BitDefender user interface is loaded at startup. This option does not affect the protection level.
Send Virus Reports	By enabling this option, virus scanning reports are sent to BitDefender labs for analysis. Please note that these reports will contain no confidential data, such as your name or IP address, and that they will not be used for commercial purposes.
Outbreak Detection	By enabling this option, reports regarding potential virus-outbreaks are sent to BitDefender labs for analysis. Please note that these reports will contain no confidential data, such as your name or IP address, and that they will not be used for commercial purposes.



12. Status Bar

As you can easily notice, in the upper part of BitDefender Antivirus 2009 window there is a status bar displaying the number of pending issues. Click the **Fix All Issues** button to easily remove any threats to your computer security. A security status window will appear.

The security status displays a systematically organized and easily manageable list of security vulnerabilities on your computer. BitDefender Antivirus 2009 will let you know whenever a problem can affect your computer's security.

	.ocal security	Monitor	Status
1	teal time file protection is enabled	✔ Yes	ОК
	You have never scanned your computer for malware	🖌 Yes	Fix
1	Jpdate performed today	🖌 Yes	ОК
- 1	Online security	Monitor	Status
	Antiphishing Protection is enabled	🖌 Yes	ОК
- 1	/ulnerability scan	Monitor	Status
	/ulnerability check is enabled	No No	Not monitored
	Eritical Microsoft updates	No No	Not monitored
	Other Microsoft updates	No No	Not monitored
	Windows Automatic Updates is enabled	No No	Not monitored
	Firefox (Out Of Date)	No	Not monitored
	Administrator (Strong Password)	No	Not monitored
	est (Weak Password)	No	Not monitored

12.1. Local security

We know it's important to be noticed whenever a problem can affect your computer's security. By monitoring each security modules, BitDefender Antivirus 2009 will let you know not only when you configure the settings that might affect your computer's security, but when you forget to do important tasks.

The issues concerning local security are described in very explicit sentences. In line with each sentence, if there is something that might affect your computer's security,



you will see a red status button called **Fix**. Otherwise, a green **OK** status button is displayed.

Issue	Description
Real time file protection is enabled	Ensures that all files are scanned as they are accessed by you or by an application running on this system.
You have scanned your computer for malware today	It is highly recommended to run an on demand scan as soon as possible to check if files stored on your computer are malware free.
Automatic update is enabled	Please keep automatic update enabled to ensure that the malware signatures of your BitDefender product are updated on a regular basis.
Updating now	Product and malware signatures update is being performed.

When the status buttons are green, the security risk of your system is at a minimum. To turn the buttons green, follow these steps:

- 1. Click the **Fix** buttons to fix security vulnerabilities one by one.
- 2. If one issue is not fixed on the spot, follow the wizard to fix it.

If you want to exclude an issue from monitoring, just clear the **Yes, monitor this component** checkbox.

12.2. Online security

The issues concerning online security are described in very explicit sentences. In line with each sentence, if there is something that might affect your computer's security, you will see a red status button called **Fix**. Otherwise, a green **OK** status button is displayed.

Issue	Description
Conversation	If your IM contacts have BitDefender 2009 installed, all IM
encryption for IM is	discussions via Yahoo! Messenger and Windows Live
enabled	Messenger will be encrypted. It is recommended to have conversation encryption for IM enabled to ensure that your IM conversations remain private.



lssue	Description
Firefox antiphishing protection is enabled	BitDefender protects you against phishing attempts when you are surfing the Internet.
Internet Explorer antiphishing protection is enabled	BitDefender protects you against phishing attempts when you are surfing the Internet.

When the status buttons are green, the security risk of your system is at a minimum. To turn the buttons green, follow these steps:

- 1. Click the **Fix** buttons to fix security vulnerabilities one by one.
- 2. If one issue is not fixed on the spot, follow the wizard to fix it.

If you want to exclude an issue from monitoring, just clear the **Yes, monitor this component** checkbox.

12.3. Vulnerability scan

The issues concerning vulnerabilities are described in very explicit sentences. In line with each sentence, if there is something that might affect your computer's security, you will see a red status button called **Fix**. Otherwise, a green **OK** status button is displayed.

Issue	Description
Vulnerability check is enabled	Monitors Microsoft Windows Updates, Microsoft Windows Office Updates and Microsoft Windows accounts passwords to ensure that your OS is up to date and is not vulnerable to password bypass.
Critical Microsoft updates	Install available critical Microsoft updates.
Other Microsoft updates	Install available non-critical Microsoft updates.



Issue	Description
Windows Automatic Updates is enabled	Install new Windows security updates as soon as they become available.
Admin (Strong Password)	Indicates the password's strength for specific users.

When the status buttons are green, the security risk of your system is at a minimum. To turn the buttons green, follow these steps:

- 1. Click the Fix buttons to fix security vulnerabilities one by one.
- 2. If one issue is not fixed on the spot, follow the wizard to fix it.

If you want to exclude an issue from monitoring, just clear the **Yes, monitor this component** checkbox.



13. Registration

BitDefender Antivirus 2009 comes with 30-day trial period. If you want to register BitDefender Antivirus 2009, to change the license key or to create a BitDefender account, click the **Register** link, located at the bottom of the BitDefender window. The registration wizard will appear.

13.1. Step 1/1 - Register BitDefender Antivirus 2009



You can see the BitDefender registration status, the current license key and how many days are left until the license expires.

To register BitDefender Antivirus 2009:

- 1. Select I want to register the product with a new key.
- 2. Type the license key in the edit field.





Note

- You can find your license key:
- on the CD label.
- on the product registration card.
- in the online purchase e-mail.

If you do not have a BitDefender license key, click the provided link to go to the BitDefender online store and buy one.

Click Finish.



14. History

The **History** link at the bottom of the BitDefender Security Center window opens another window with the BitDefender history & events. This window offers you an overview of the security-related events. For instance, you can easily check if the update was successfully performed, if malware was found on your computer etc.

			_ ×
Module			
Update			
Name of the action	Action Taken	Date and time	^
Downloaded files	The update files wer	7/17/2008 4:08:29 PM	
 Update success 	The engine and signa	7/17/2008 4:08:29 PM	
Update success	The engine and signa	7/17/2008 4:08:29 PM	
🌐 Update success	The engine and signa	7/17/2008 3:08:28 PM	
Downloaded files	The update files wer	7/17/2008 3:08:28 PM	
Update success	The engine and signa	7/17/2008 3:08:28 PM	
Downloaded files	The update files wer	7/17/2008 2:08:39 PM	
Update success	The engine and signa	7/17/2008 2:08:39 PM	
Update success	The engine and signa	7/17/2008 2:08:39 PM	
🌡 Update success	The engine and signa	7/17/2008 11:57:45 AM	
Downloaded files	The update files wer	7/17/2008 11:57:45 AM	
Update success	The engine and signa	7/17/2008 11:57:45 AM	
Downloaded files	The update files wer	7/16/2008 7:01:36 PM	
Update success	The engine and signa	7/16/2008 7:01:36 PM	
Update success	The engine and signa	7/16/2008 7:01:36 PM	
Downloaded files	The update files wer	7/15/2008 9:42:49 PM	
Update success	The engine and signa	7/15/2008 9:42:49 PM	
Update success	The engine and signa	7/15/2008 9:42:49 PM	
Update success	The engine and signa	7/15/2008 8:42:44 PM	
Downloaded files	The update files wer	7/15/2008 8:42:44 PM	
Update success	The engine and signa	7/15/2008 8:42:44 PM	~
	Vodule Update Update Name of the action Durnloaded files Update success Update success Downloaded files Update success Update succes Update success Update success	Update Update Name of the action Action Taken I Downloaded files The update files wer Update success The engine and signa Update success The engine and signa Update success The engine and signa I Update success The engine and signa	Update Update 7/17/2008 4:08:29 PM I Downloaded files The update files wer 7/17/2008 4:08:29 PM I Update success The engine and signa 7/17/2008 4:08:29 PM I Update success The engine and signa 7/17/2008 4:08:29 PM I Update success The engine and signa 7/17/2008 4:08:29 PM I Update success The engine and signa 7/17/2008 3:08:28 PM I Downloaded files The update files wer 7/17/2008 3:08:28 PM I Update success The engine and signa 7/17/2008 2:08:39 PM I Update success The engine and signa 7/17/2008 2:08:39 PM I Update success The engine and signa 7/17/2008 2:08:39 PM I Update success The engine and signa 7/17/2008 1:157:45 AM I Update success The engine and signa 7/17/2008 1:157:45 AM I Update success The engine and signa 7/16/2008 7:01:36 PM I Update success The engine and signa 7/16/2008 7:01:36 PM I Update success The engine and signa 7/16/2008 7:01:36 PM I Update success The engine

In order to help you filter the BitDefender history & events, the following categories are provided on the left side:

- Antivirus
- Privacy Control
- Update
- Network

A list of events is available for each category. Each event comes with the following information: a short description, the action BitDefender took on it when it happened,



and the date and time when it occurred. If you want to find out more information about a particular event in the list, double click that event.

Click **Clear Log** if you want to remove old logs or **Refresh** to make sure the latest logs are displayed.



Advanced Administration



15. General

The General module provides information on the BitDefender activity and the system. Here you can also change the overall behavior of BitDefender.

15.1. Dashboard

To see product activity statistics and your registration status, go to **General>Dashboard** in the Advanced View.

BitDefender Antivir	us 2009 - Trial			SWITC	H TO BASIC VIEW
STATUS: There is 1 pend	ing issue				FIX ALL ISSUES
	Dashboard Se	ttings SysInfo			
General					
Antivirus	Statistics		_	Overview	
Privacy Control	Scanned files:	359	3	Last update:	//1//2008 4:08 PM
Vulnerability	Disinfected files:	1	0	MyAccount:	No account
Encryption	Detected viruses:	1	0	Registration:	trial version
Network				Expires in:	
Update					30 days left
Registration	Filezone				
Q					
(Spitdefender)				My Account - Register	- <u>Help</u> - <u>Support</u> - <u>History</u>
Dashboard					

The dashboard consists of several sections:

- Statistics Displays important information regarding the BitDefender activity.
- **Overview** Displays the update status, your account status, registration and license information.



■ **Filezone** - Indicates the evolution of the number of objects scanned by BitDefender Antimalware. The height of the bar indicates the intensity of the traffic during that time interval.

15.1.1. Statistics

If you want to keep an eye on the BitDefender activity, a good place to start is the Statistics section. You can see the following items:

Item	Description
Scanned files	Indicates the number of files that were checked for malware at the time of your last scan.
Disinfected files	Indicates the number of files that were disinfected at the time of your last scan.
Detected viruses	Indicates the number of viruses that were found on your system at the time of your last scan.

15.1.2. Overview

This is where you can see a summary of statistics regarding the update status, your account status, registration and license information.

Item	Description
Last update	Indicates the date when your BitDefender product was last updated. Please perform regular updates in order to have a fully protected system.
My account	Indicates the e-mail address that you can use to access your on-line account to recover your lost BitDefender license key and to benefit from BitDefender support and other customized services.
Registration	Indicates your license key type and status. To keep your system safe you must renew or upgrade BitDefender if your key has expired.
Expires in	Indicates the number of days left until the license key expires.



15.2. Settings

To configure general settings for BitDefender and to manage its settings, go to **General>Settings** in the Advanced View.

BitDefender Antivir	SWITCH TO BASIC VIEW	
STATUS: There are 2 pen	ding issues	FIX ALL ISSUES
	Dashboard Settings SysInfo	
General		
Antivirus	General Settings	
Privacy Control	Enable password protection for product settings	
Vulnerability	Show BitDefender News (security related notifications)	
Encryption	Show pop-ups (on-screen notes)	
Network	Show popups in Advanced View	
Update	Show popups in Basic View	
Registration	Load BitDefender at Windows startup	
	Virus Report Settings	
Q		
Ebitdefender	My Account	: - <u>Register</u> - <u>Help</u> - <u>Support</u> - <u>History</u>
General 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.

15.2.1. General Settings

■ Enable password protection for product settings - enables setting a password in order to protect the BitDefender 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 following window will appear:

Bit Defender		x
You must enter a password and retype it to confirm.		
The password should be a	at least 8 characters long,	
Password		
Retype password		
	OK Cancel	

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

Once you have set the password, you will be asked for it whenever you want to change the BitDefender settings. The other system administrators (if any) will also have to provide this password in order to change the BitDefender settings.



Enter 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. You can configure BitDefender to display pop-ups only when using the Basic View or the Advanced View.
- Load BitDefender at Windows startup automatically launches BitDefender at system startup. We recommend you to keep this option selected.
- Enable the Scan Activity bar (on screen graph of product activity) displays the Scan Activity bar whenever you log on to Windows. Clear this check box if you do not want the Scan Activity bar to be displayed anymore.



This option can be configured only for the current Windows user account.

15.2.2. Virus Report Settings

Note

■ 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.

15.3. System Information

BitDefender allows you to view, from a single location, all system settings and the applications registered to run at startup. In this way, you can monitor the activity of the system and of the applications installed on it as well as identify possible system infections.

To obtain system information, go to General>System Info in the Advanced View.

BitDefender Antiviru	ıs 2009 - Trial	SWITCH TO BASIC VIEW
STATUS: There are 2 pend	ing issues	FIX ALL ISSUES
	Dashboard Settings SysInfo	
General		
Antivirus	Current System Settings	
Privacy Control	Run Items (9) Start In Items (2)	<u>^</u>
Vulnerability	■ Load Items (5)	
Encryption	Userinit (1) EUWINDOWSkauster 22/userinit eve	-
Network	Current User Shell (Item not found)	
Update	Local Machine Shell (1) Application July DL c (2)	
Registration	Winlogon Notify (9) Winlogon Notify (9) INI Items (2) Known DLLs (21)	
	 File Associations (8) ■ Scripts (2) 	v
	Selected Item Description	
	Programs that run at startup or after a user logs in. These settings are located in the registry.	
		×
		Refresh
Q		
(Spitdefender)		<u>My Account</u> - <u>Register</u> - <u>Help</u> - <u>Support</u> - <u>History</u>
System Informatio	n	

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

Three buttons are available:

- Restore changes a current file association to default. Available for the File Associations settings only!
- Go to opens a window where the selected item is placed (the Registry for example).



Note

Depending on the selected item, the Go to button may not appear.

Refresh - re-opens the System Info section.



16. Antivirus

BitDefender protects your computer from all kinds of malware (viruses, Trojans, spyware, rootkits and so on). The protection BitDefender offers is divided into two categories:

Real-time protection - prevents new malware threats from entering your system. BitDefender will, for example, scan a word document for known threats when you open it, and an e-mail message when you receive one.



Note

Real-time protection is also referred to as on-access scanning - files are scanned as the users access them.

On-demand scanning - allows detecting and removing the malware that already resides in the 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. The scan tasks allow you to create customized scanning routines and they can be scheduled to run on a regular basis.

16.1. Real-time Protection

BitDefender provides continuous, real-time protection against a wide range of malware threats by scanning all accessed files, e-mail messages and the communications through Instant Messaging Software applications (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). BitDefender Antiphishing prevents you from disclosing personal information while browsing the Internet by alerting you about potential phishing web pages.

To configure real-time protection and BitDefender Antiphishing, go to **Antivirus>Shield** in the Advanced View.



BitDefender Antiv	irus 2009 - Trial Switch to Basic View
STATUS: There are 2 pe	nding issues FIX ALL ISSUES
	Shield Virus Scan Excludes Quarantine
General	
Antivirus	✓ Real-time protection is enabled
Privacy Control	Last system scan: never
Vulnerability	Scan Now
Encryption	Protection Level
Network	
Update	DEFAULT -Standard security, low use of resources Aggressive -Scap all files (includes network scap)
Registration	
Q	
(Spitdefender)	My Account - Realister - Help - Susport - History
Real-time Protect	ction

You can see whether Real-time protection is enabled or disabled. If you want to change the Real-time protection status, clear or select the corresponding check box.



Important

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

To start a quick system scan, click **Scan Now**.

16.1.1. Configuring 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	Covers basic security needs. The resource consumption level is very low.
	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.
Default	Offers standard security. The resource consumption level is low.
	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.
Aggressive	Offers high security. The resource consumption level is moderate.
	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.

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

16.1.2. Customizing Protection Level

Advanced users might want to take advantage of the scan settings BitDefender offers. The scanner can be set to scan only specific file extensions, to search for specific malware threats or to skip archives. This may greatly reduce scanning times and improve your computer's responsiveness during a scan.

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





Shield Settings

The scan options are organized as an expandable menu, very similar to those used for exploration in Windows. Click the box with "+" to open an option or the box with "-" to close an option.



Note

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;

BitDefender Antivirus 2009

Option		Description	
		<pre>.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.</pre>	
	Scan user defined extensions	Only the files with the extensions specified by the user will be scanned. These extensions must be separated by ";".	
	Scan for riskware	Scans for riskware. Detected files will be treated as infected. The 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 boot		Scans the system's boot sector.	
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 infected files.	
	Delete file	Deletes infected files immediately, without any warning.	
	Move file to quarantine	Moves infected files into the quarantine.	

Option			Description
Second action			Select from the drop-down menu the second action to take on infected files, in case the first action fails.
	Deny access continue	and	In case an infected file is detected, the access to this will be denied.
	Delete file		Deletes infected files immediately, without any warning.
	Move file quarantine	to	Moves infected files into the quarantine.
Do not scan Kb	files greater tha	an [x]	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.
Do not scan archives greater than [20000] Kb		ər	Type in the maximum size of the archives to be scanned in kilobytes (KB). If you want to scan all archives, regardless of their size, type 0.
Do not scan network shares		6	If this option is enabled, BitDefender will not scan the network shares, allowing for a faster network access.
			We recommend you to enable this option only if the network you are part of is protected by an antivirus solution.

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.

Scan files received/sent over IM. To scan the files you receive or send using Yahoo Messenger or Windows Live Messenger, select the corresponding check boxes.

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

16.1.3. Configuring the Behavioral Scanner

The Behavioral Scanner provides a layer of protection against new threats for which signatures have not yet been released. It constantly monitors and analyses the behavior of the applications running on your computer and alerts you if an application has a suspicious behavior.

The Behavioral Scanner alerts you whenever an application tries to perform a possible malicious action and prompts you for action.



If you know and trust the detected application, click **Allow**. The Behavioral Scanner will no longer scan the application for possible malicious behavior.

If you want to immediately close the application, click OK.

Behavioral Scanner Alert

To configure the Behavioral Scanner, click Scanner Settings.



Denational	Scanner is enabled.
- Critical High - Medium - Low	Applications are intensely monitored for possible malicious actions
xcluded App	lications

Behavioral Scanner Settings

If you want to disable the Behavioral Scanner, clear the **Behavioral Scanner is** enabled check box.



Important

Keep the Behavioral Scanner enabled in order to be protected against unknown viruses.

Configuring the Protection Level

The Behavioral Scanner protection level automatically changes when you set a new real-time protection level. If you are not satisfied with the default setting, you can manually configure the protection level.



Note

Keep in mind that if you change the current real-time protection level, the Behavioral Scanner protection level will change accordingly.

Drag the slider along the scale to set the protection level that best fits your security needs.

Protection level	Description
Critical	Applications are strictly monitored for possible malicious actions.
High	Applications are intensely monitored for possible malicious actions.
Medium	Applications are moderately monitored for possible malicious actions.
Low	Applications are monitored for possible malicious actions.

Managing Excluded Applications

You can configure the Behavioral Scanner not to check specific applications. The applications that are not currently checked by the Behavioral Scanner are listed in the **Excluded Applications** table.

To manage the excluded applications, you can use the buttons placed at the top of the table:

- ■ Add exclude a new application from scanning.
- **Remove** remove an application from the list.
- **Edit** edit an application path.

16.1.4. Disabling Real-time Protection

If you want to disable real-time protection, a warning window will appear.



You must confirm your choice by selecting from the menu how long you want the real-time protection to be disabled. You can disable real-time protection for 5, 15 or 30 minutes, for an hour, permanently or until the system restart.



Warning

This is a critical security issue. We recommend you to disable real-time protection for as little time as possible. If real-time protection is disabled, you will not be protected against malware threats.

16.1.5. Configuring Antiphishing Protection

BitDefender provides real-time antiphishing protection for:

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

You can choose to disable the antiphishing protection completely or for specific applications only.

You can click **White List** to configure and manage a list of web sites that should not be scanned by BitDefender Antiphishing engines.

BitDefender - Antiphishing	×
White List	
This is the list of urls that will not be processed by our engines.	
The URLs entered in the Whitelist will not be checked by the BitDefender You will not be notified about any threats existing on these pages.	Antiphishing engines.
New address	Add
Website	
www.amazon.com	Remove
	v
C This is where you can define a list of websites (URLs) that should not be checked by I engines.	BitDefender Antiphishing
	Save Close
Antiphishing White List	

You can see the web sites that BitDefender does not currently check for phishing content.



To add a new web site to the white list, type its url address in the **New address** field and click **Add**. The white list should contain only web sites you fully trust. For example, add the web sites where you currently shop online.



Note

You can easily add web sites to the white list from the BitDefender Antiphishing toolbar integrated into your web browser.

If you want to remove a web site from the white list, click the corresponding **Remove** button.

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

16.2. On-demand Scanning

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.

To configure and initiate on-demand scanning, go to **Antivirus>Scan** in the Advanced View.

BitDefender Antivi	rus 2009 - Trial	SWITCH TO BASIC VIEW
STATUS: There are 2 per	nding issues	FIX ALL ISSUES
	Shield Virus Scan Exclud	les Quarantine
General	System tasks	
Antivirus	Deep System Scan	
Privacy Control	Last Run: Never	
Vulnerability	Full System Scan	
Encryption	Quick System Scan	
Network	Last Run: Never	
Update	Autologon Scan	
Registration	User tasks	
	My Documents Last Run: Never Misc tasks Contextual Scan Contextual Scan Device detection	Rew Task Run Task
Q		
(Spitdefender)		My Account - Register - Help - Support - History
Scan Tasks		

On-demand scanning is based on scan tasks. Scan tasks specify the scanning options and the objects to be scanned. You can scan the computer whenever you want by running the default tasks or your own scan tasks (user-defined tasks). You can also schedule them to run on a regular basis or when the system is idle so as not to interfere with your work

16.2.1. Scan Tasks

BitDefender comes with several tasks, created by default, which cover common security issues. You can also create your own customized scan tasks.

Each task has a **Properties** window that allows you to configure the task and to see the scan results. For more information, please refer to "*Configuring Scan Tasks*" (p. 110).

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. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.
Full System Scan	Scans the entire system, except for archives. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.
Quick System Scan	Scans the Windows, Program Files and All Users folders. In the default configuration, it scans for all types of malware, except for rootkits, but it does not scan memory, the registry or cookies.
Autologon Scan	Scans the items that are run when a user logs on to Windows. By default, the autologon scan is disabled.
	If you want to use this task, right-click it, select Schedule and set the task to run at system startup . You can specify how long after the startup the task should start running (in minutes).



Note

Since the **Deep System Scan** and **Full System Scan** tasks analyze the entire system, the scanning may take a while. Therefore, we recommend you to run these tasks on low priority or, better, when your system is idle.

User tasks - contains the user-defined tasks.

A task called My Documents is provided. Use this task to scan important current user folders: My Documents, Desktop and StartUp. This will ensure the safety of your documents, a safe workspace and clean applications running at startup.

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 indicates that the selected task is scheduled for later. Click this button to open the Properties window, Scheduler tab, where you can see the task schedule and modify it.
- **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.

To the left of each task you can see the **Properties** button, that allows you to configure the task and view the scan logs.

16.2.2. Using 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.
- Paths opens the Properties window, Paths tab, where you can change the scan target of the selected task.

System tasks					
8	Deep System Scan Last Run: Never				
8	Full System Scan Last Run: 7/16/2008 12:17:22	PM			
6	Quick System Scan				
8	Autologon Scan Last Run: 5/9/2008 7:16:42 P	м			
User ta	iks				
C	My Documents Last Run: Never	Scan Now	1	٦	2 5
Misc tas	iks				
8	Contextual Scan	Change Scan Target Schedule Task View Scan Logs			
6	Device detection	Duplicate Delete			
		Properties			
Shortcut Menu					



Note

In the case of system tasks, this option is replaced by **Show Task Paths**, as you can only see their scan target.

Schedule - opens the Properties window, Scheduler tab, where you can schedule the selected task.



- Logs opens the Properties window, Logs tab, where you can see the reports generated after the selected task was run.
- Clone duplicates the selected task. This is useful when creating new tasks, as you can modify the settings of the task duplicate.
- Delete deletes the selected task.



Note

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

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



Note

Due to the particular nature of the ${\rm Misc}$ Tasks category, only the ${\rm Logs}$ and ${\rm Open}$ options are available in this case.

16.2.3. Creating Scan Tasks

To create a scan task, use one of the following methods:

- 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.

16.2.4. Configuring Scan Tasks

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 open this window click the **Open** button, located on the right of the task (or right-click the task and then click **Open**).



Note

For more information on viewing logs and the **Logs** tab, please refer to "*Viewing Scan Logs*" (p. 129).

Configuring Scan Settings

To configure the scanning options of a specific scan task, right-click it and select **Properties**. The following window will appear:



Overview Paths Scheduler Logs Task properties Task name: Desktop	tDefender - Ne	ew Task		3
Task properties Task name: Desistop Last Rum: never Scheduld: No Scanning options Hah MEDIUM - Recommended for most users - Scan all files - Scan all files - Scan for Viruses and spyware Low Custom Default Run the task with low priority Minimize to tray Shut down computer when scan completes if no threats are found Image: This is where the main characteristics of a new scan task, including scannic level, can be defined. Scan OK	Overview	Paths	Scheduler	Logs
Task name: Desktop Lask Rum never Scheduled: No Scheduled: No Scanning options High Medium Custom Run the task with low priority Minimize to tray Shut down computer when scan completes if no threats are found This is where the main characteristics of a new scan task, including scanni level, can be defined. Scan OK Cancel	Task properties			
Last Rum: never Scheduled: No Scanning options High Medium - Scan all files -	Task name: Desktop	4]
Scheduled: No Scanning options Hah Medium Hah Medium Custom Default Run the task with low priority Minimize to tray Shut down computer when scan completes if no threats are found This is where the main characteristics of a new scan task, including scanni level, can be defined. Custom OK Cancel	Last Run: never			
Scanning options High High High Custom Custom Custom Custom Custom Perfault Shut down computer when scan completes if no threats are found This is where the main characteristics of a new scan task, including scannin level, can be defined. Custom C	Scheduled: No			
Hah MEDIUM - Recommended for most users - Scan al files - Scan al files - Scan for Viruses and spyware - Low Custom Default - Minimize to tray - Shut down computer when scan completes if no threats are found - This is where the main characteristics of a new scan task, including scannic - This is where the main characteristics of a new scan task, including scannic - Scan OK Cancel	Scanning options			
Scan all files Scan for Viruses and spyware Low Custom Default Minimize to tray Shut down computer when scan completes if no threats are found This is where the main characteristics of a new scan task, including scannin level, can be defined. Scan OK Cancel	- High	MEDIUM - Re	commended for mo	st users
Low Custom Default Custom Default Minimize to tray Shut down computer when scan completes if no threats are found This is where the main characteristics of a new scan task, including scanni there, can be defined. Scan OK Cancel	Medium	- Scan all files - Scan for viru	ses and spyware	
Custom Default Run the task with low priority Minimize to tray Minimize to tray Shut down computer when scan completes if no threats are found This is where the main characteristics of a new scan task, including scannil level, can be defined. OK Cancel OK	- Low			
Run the task with low priority Minimize to tray Shut down computer when scan completes if no threats are found This is where the main characteristics of a new scan task, including scannic level, can be defined. Scan OK Cancel		Custom	Default	
Minimize to tray Shut down computer when scan completes if no threats are found This is where the main characteristics of a new scan task, including scannil level, can be defined. Scan OK	Run the task with	low priority		
Shut down computer when scan completes if no threats are found This is where the main characteristics of a new scan task, including scanni I level, can be defined. Scan OK Cancel	Minimize to tray			
This is where the main characteristics of a new scan task, including scanni level, can be defined. Scan OK Cancel	Shut down comput	er when scan com	pletes if no threats	are found
In the owner of the near Characteristics of a new scart case, including scarming level, can be defined. Scan OK Cancel	This is subset to			
Scan OK Cancel	R level, can be de	efined.	uus or a new suarru	ask, including scanning
	Scan		ОК	Cancel
· · · · · · · · · · · · · · · · · · ·				

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

Choosing Scan Level

You can easily configure the scan settings by choosing the scan level. Drag the slider along the scale to set the appropriate scan level.

There are 3 scan levels:

Protection level	Description
Low	Offers reasonable detection efficiency. The resource consumption level is low.
	Programs only are scanned for viruses. Besides the classical signature-based scan, the heuristic analysis is also used.
Medium	Offers good detection efficiency. The resource consumption level is moderate.
	All files are scanned for viruses and spyware. Besides the classical signature-based scan, the heuristic analysis is also used.



Protection level	Description
High	Offers high detection efficiency. The resource consumption level is high.
	All files and archives are scanned for viruses and spyware. Besides the classical signature-based scan, the heuristic analysis is also used.

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

- Run the task with Low priority. Decreases the priority of the scan process. You will allow other programs to run faster and increase the time needed for the scan process to finish.
- Minimize scan window on start to systray. Minimizes the scan window to the system tray. Double-click the BitDefender icon to open it.
- Shut down the computer when scan completes if no threats are found

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

Customizing Scan Level

Advanced users might want to take advantage of the scan settings BitDefender offers. The scanner can be set to scan only specific file extensions, to search for specific malware threats or to skip archives. This may greatly reduce scanning times and improve your computer's responsiveness during a scan.

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



Scan Settings

The scan options are organized as an expandable menu, very similar to those used for exploration in Windows. Click the box with "+" to open an option or the box with "-" to close an option.

The scan options are grouped into 3 categories:

■ Scan Level. Specify the type of malware you want BitDefender to scan for by selecting the appropriate options from the Scan Level category.

Option	Description	
Scan for viruses	Scans for known viruses.	
	BitDefender detects incomplete virus bodies, too, thus removing any possible threat that could affect your system's security.	
Scan for adware	Scans for adware threats. Detected files will be treated as infected. The software that includes adware components might stop working if this option is enabled.	

Option	Description	
Scan for spyware	Scans for known spyware threats. Detected files will be treated as infected.	
Scan for application	Scan for legitimate applications that can be used as a spying tool, to hide malicious applications or for other malicious intent.	
Scan for dialers	Scans for applications dialing high-cost numbers. Detected files will be treated as infected. The software that includes dialer components might stop working if this option is enabled.	
Scan for rootkits	Scans for hidden objects (files and processes), generally known as rootkits.	

Virus scanning options. Specify the type of objects to be scanned (file types, archives and so on) by selecting the appropriate options from the Virus scanning options category.

Option		Description
Scan files	Scan all files	All files are scanned, regardless of their type.
	Scan program files only	Only the program files will be scanned. This means only the files with the following extensions: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; 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 ";".
Open packed programs		Scans packed files.
Open archives		Scans inside archives.



Option	Description
	Scanning archived files increases the scanning time and requires more system resources. You can click the Archive size limit field and type the maximum size of the archives to be scanned in kilobytes (KB).
Open e-mail archives	Scans inside mail archives.
Scan boot sectors	Scans the system's boot sector.
Scan memory	Scans the memory for viruses and other malware.
Scan registry	Scans registry entries.
Scan cookies	Scans cookie files.

■ Action options. Specify the action to be taken on the each category of detected files using the options in the Action options category.



Note

To set a new action, click the current action and select the desired option from the menu.

• Select the action to be taken on the infected files detected. The following options are available:

Action	Description	
None (log objects)	No action will be taken on infected files. These files will appear in the report file.	
Disinfect files	Remove the malware code from the infected files detected.	
Delete files	Deletes infected files immediately, without any warning.	
Move files to Quarantine	Moves infected files into the quarantine. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.	



• Select the action to be taken on the suspicious files detected. The following options are available:

Action	Description
None (log objects)	No action will be taken on suspicious files. These files will appear in the report file.
Delete files	Deletes suspicious files immediately, without any warning.
Move files to Quarantine	Moves suspicious files into the quarantine. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.



Note

Files are detected as suspicious by the heuristic analysis. We recommend you to send these files to the BitDefender Lab.

• Select the action to be taken on the hidden objects (rootkits) detected. The following options are available:

Action	Description
None (log objects)	No action will be taken on hidden files. These files will appear in the report file.
Move files to Quarantine	Moves hidden files into the quarantine. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.
Make visible	Reveals hidden files so that you can see them.

- Archived files action options. Scanning and handling files inside archives are subject to restrictions. Password-protected archives cannot be scanned unless you provide the password. Depending on the archive format (type), BitDefender may not be able to disinfect, isolate or delete infected archived files. Configure the actions to be taken on the archived files detected using the appropriate options from the Archived files action options category.
 - $\circ\,$ Select the action to be taken on the infected files detected. The following options are available:



Action	Description
Take no action	Only keep record of infected archived files in the scan log. After the scan is completed, you can open the scan log to view information on these files.
Disinfect files	Remove the malware code from the infected files detected. Disinfection may fail in some cases, such as when the infected file is inside specific mail archives.
Delete files	Immediately remove infected files from the disk, without any warning.
Move files to Quarantine	Move infected files from their original location to the quarantine folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.

 $\circ\,$ Select the action to be taken on the suspicious files detected. The following options are available:

Action	Description	
Take no action	Only keep record of suspicious archived files the scan log. After the scan is completed, yo can open the scan log to view information of these files.	
Delete files	Deletes suspicious files immediately, without any warning.	
Move files to Quarantine	Moves suspicious files into the quarantine. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears.	

 $\circ\,$ Select the action to be taken on the password-protected files detected. The following options are available:



Action	Description
Log as not scanned	Only keep record of the password-protected files in the scan log. After the scan is completed, you can open the scan log to view information on these files.
Prompt for password	When a password-protected file is detected, prompt the user to provide the password in order to scan the file.



Note

If you choose to ignore the detected files or if the chosen action fails, you will have to choose an action in the scanning wizard.

If you click $\ensuremath{\text{Default}}$ you will load the default settings. Click $\ensuremath{\text{OK}}$ to save the changes and close the window.

Setting Scan Target

To set the scan target of a specific user scan task, right-click the task and select **Paths**. The following window will appear:



BitDefender - N	ew Task		×
Overview	Paths	Scheduler	Logs
31/3 Floppy 1 Tr (C:) 22k (D:) 22k (D:)	(A:) 5:) ts and Settings\tesl	\Desktop	Local Drives
©. Scan		OK	Add folder(s) Delete item(s) Cancel

Scan Target

You can see the list of local, network and removable drives as well as the files or folders added previously, if any. All checked items will be scanned when running the task.

The section contains the following buttons:

Add Items(s) - opens a browsing window where you can select the file(s) / folder(s) that you want to be scanned.



Note

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

Remove Item(s) - removes the file(s) / folder(s) 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 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, select the checkbox corresponding to $\ensuremath{\text{AII}}$ Entries.

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

Viewing the Scan Target of System Tasks

You can not modify the scan target of the scan tasks from the **System Tasks** category. You can only see their scan target.

To view the scan target of a specific system scan task, right-click the task and select **Show Task Paths**. For **Full System Scan**, for example, the following window will appear:



Scan Target of Full System Scan



Full System Scan and Deep System Scan will scan all local drives, while Quick System Scan will only scan the Windows and Program Files folders.

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

Scheduling Scan Tasks

With complex tasks, the scanning process will take some time and it will work best if you close all other programs. That is 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.

To see the schedule of a specific task or to modify it, right-click the task and select **Schedule Task**. The following window will appear:

Overview Paths Scheduler Logs Properties Scheduled: daily, next scan:7/17/2008 11:21:07 PM O no: O no: O no: Periodically O n system startup At every: Image: Start date: 7/17/2006 Start date: 7/17/2006 Start time: 11:21:07 PM	SitDefender -	New Task		×
Properties Schedule: daily, next scan:7/17/2008 11:21:07 PM Once Periodcally On system startup At every: 1 @ days V Start date: 7/17/2008 V Start time: 11:21:07 PM \$	Overview	Paths	Scheduler	Logs
Scheduled: daily, next scan:7/17/2008 11:21:07 PM Schedule Once Periodcally On system startup At every: 1 @ days Start date: 7/17/2008 Start time: 11:21:07 PM Start time: 11:21:07 PM Scan OK Cancel	Properties			
Schedule No Once Periodically On system startup At every: 1 days v Start date: 7/17/2008 v Start date: 11:21:07 PM ¢ Scan OK Cancel	Scheduled: daily,	next scan:7/17/2008	11:21:07 PM	
No Once Periodcally On system startup At every: 1	Schedule			
 Once Periodically On system startup: At every: 1	O No			
Periodcally On system starup At every: Start date: 7/17/2008 Start time: 11:21:07 PM Start time: Scan OK Cancel Chadular Cancel Cancel	Once			
On system startup At every: 1 @ days Start date: 7/17/2008 Start time: 11:21:07 PM Scan OK Cancel Chadular	Periodically			
At every: 1 days v Start date: 7/17/2008 v Start time: 11:21:07 PM ÷	 On system st 	artup		
Start date: 7/17/2006 Start time: 11:21:07 PM Start time: 11:21:07 PM Start time: 0K Cancel	At every:	1 🗘 days	~	
Start time: 11:21:07 PM 🖨	Start date:	7/17/2008		
Cancel	Start time:	11:21:07 PM		
Scan OK Cancel				
Scan OK Cancel				
Cancel				
Scan OK Cancel choolulor				
Scan OK Cancel	0			
Scan OK Cancel	U 1			
cheduler	Scan		ОК	Cancel
cheduler				
	chodulor			

You can see the task schedule, if any.

When scheduling a task, you must 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.

On system startup - launches the scan at the specified number of minutes after a user has logged on to Windows.

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

16.2.5. Scanning Objects

Before you initiate a scanning process, you should make sure that BitDefender is up to date with its malware signatures. Scanning your computer using an outdated signature database may prevent BitDefender from detecting new malware found since the last update. To verify when the last update was performed, click **Update>Update** in the settings console.



Note

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.

Scanning Methods

BitDefender provides four types of on-demand scanning:

- Immediate scanning run a scan task from the system / user tasks.
- Contextual scanning right-click a file or a folder and select BitDefender Antivirus 2009.
- Drag&Drop scanning drag and drop a file or a folder over the Scan Activity Bar.
- Manual scanning use BitDefender Manual Scan to directly select the files or folders to be scanned.

Immediate Scanning

To scan your computer or part of it you can run the default scan tasks or your own scan tasks. This is called immediate scanning.

To run a scan task, use one of the following methods:



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

The BitDefender Scanner will appear and the scanning will be initiated. For more information, please refer to "*BitDefender Scanner*" (p. 125).

Contextual Scanning

To scan a file or a folder, without configuring a new scan task, you can use the contextual menu. This is called contextual scanning.



Right-click the file or folder you want to be scanned and select **BitDefender Antivirus 2009**.

The BitDefender Scanner will appear and the scanning will be initiated. For more information, please refer to *"BitDefender Scanner"* (p. 125).

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 to be scanned and drop it over the **Scan Activity Bar** as shown below.





The BitDefender Scanner will appear and the scanning will be initiated. For more information, please refer to "*BitDefender Scanner*" (p. 125).

Manual Scanning

Manual scanning consists in directly selecting the object to be scanned using the BitDefender Manual Scan option from the BitDefender program group in the Start Menu.



Note

Manual scanning is very useful, as it can be performed when Windows works in Safe Mode, too.

To select the object to be scanned by BitDefender, in the Windows Start menu, follow the path Start \rightarrow Programs \rightarrow BitDefender 2009 \rightarrow BitDefender Manual Scan. The following window will appear:



Browse for Folder	? 🗙
Please select the scan target.	
My Consultat 376 Floppy (A;) Social Disk (C;) Coal Di	► ►
OK Cano	*
Manual Scanning	

Choose the object that you want to be scanned and click $\ensuremath{\textbf{OK}}$.

The BitDefender Scanner will appear and the scanning will be initiated. For more information, please refer to "*BitDefender Scanner*" (p. 125).

BitDefender Scanner

When you initiate an on-demand scanning process, the BitDefender Scanner will appear. Follow the three-step guided procedure to complete the scanning process.

Step 1/3 - Scanning

BitDefender will start scanning the selected objects.

Ditberender 2003	- Full System Scan		_ ×
Antivirus Scan - Step	1 of 3		
	Step1	Step2	Step
Scan Status			
Current Scanned Item	=>HKEY_LOCAL_MACHINE\SYSTE	4\CURRENTth=>C:\WINDOWS\SYSTEM32\DRIVER	RS\BDFSFLTR.SYS
Elapsed Time:	00:00:03		
Files/Second:	8		
Scan Statistics			
Scanned Items:	24		
Not Scanned Items:	0		
Infected Items:	0		
Suspect Items:	0		
Hidden Items:	0		
Hidden Processes:	0		
Antivirus scanning in p	rogress. The section above indicates the pr	gress of and the section below statistics on this proc	tess. By default,
C Antivirus scanning in p BitDefender will try to	rogress. The section above indicates the pr disinfect the items detected as infected.	ogress of and the section below statistics on this proc	cess. By default,

You can see the scan status and statistics (scanning speed, elapsed time, number of scanned / infected / suspicious / hidden objects and other).



Note

The scanning process may take a while, depending on the complexity of the scan.

To temporarily stop the scanning process, just click **Pause**. You will have to click **Resume** to resume scanning.

You can stop scanning anytime you want by clicking **Stop&Yes**. You will go directly to the last step of the wizard.

Wait for BitDefender to finish scanning.

Step 2/3 - Select Actions

When the scanning is completed, a new window will appear, where you can see the scan results.



BitDefender 2009 - Full System Scan		_ ×
Antivirus Scan - Step 2 of 3		
Step1	Step2	Step3
Results Summary		
126 threat(s) that affected 243 object(s) require(s) ye	our attention	Take no action
Generic.Peed.Eml.071B72F7	2 issues left (disinfection failed)	Take no action 💌 🔺
Generic.Peed.Eml.0A3EE9A2	2 issues left (disinfection failed)	Take no action 💌
Generic.Peed.Eml.0B4D1482	2 issues left (disinfection failed)	Take no action 💌
Generic.Peed.Eml.0CE75927	2 issues left (disinfection failed)	Take no action
Generic.Peed.Eml.10087D60	2 issues left (disinfection failed)	Take no action
Generic.Peed.Eml.10D5AEE5	2 issues left (disinfection failed)	Take no action 💌 👻
Solved issues count: 4		
File path	Threat name	Action result
E:\kituri\kituri on home (cWhereisit 3.51\WhereIsIt.exe	Backdoor.Bot.15122	deleted
E:\System Volume Informatio72B5CB0D}\RP260\A0069234.exe	Backdoor.Bot.15122	deleted
E:\muzica\scrisa\dvd1(scris)\OPM 2.7\Loader\launch.exe	Trojan.Generic.227562	deleted
E:\System Volume Informatio7285CB0D}\RP260\A0069235.exe	Trojan.Generic.227562	deleted
R BitDefender has detected and blocked viruses on your computer list of infected items.	! This is the list of threats. Please click the vi	rus name to see its corresponding
(Spitdefender)		Continue
Actions		

You can see the number of issues affecting your system.

The infected objects are displayed in groups, based on the malware they are infected with. Click the link corresponding to a threat to find out more information about the infected objects.

You can choose an overall action to be taken for all issues or you can select separate actions for each group of issues.

The following options can appear on the menu:

Action	Description
Take No Action	No action will be taken on the detected files.
Disinfect	Disinfects infected files.
Delete	Deletes detected files.
Unhide	Makes hidden objects visible.



Click **Continue** to apply the specified actions.

Step 3/3 - View Results

When BitDefender finishes fixing the issues, the scan results will appear in a new window.

BitDefender 200	9 - Full Syste	m Scan	_ ×
Antivirus Scan - Ste	p 3 of 3		
	Step 1	Step2	Step 3
Results Summary			
Resolved Items:	4		
Unresolved Items:	243		
Password Protected Ite	ems: 0		
Ignored Items:	0		
Failed Items:	243		
Antivirus scanning co	mpleted. These are th	e statistics of this scan task.	
(Spitdefender)			Show Log File Close
Summary			

You can see the results summary. Click Show log file to view the scan log.

Important If required, please restart your system in order to complete the cleaning process.

Click Close to close the window.

BitDefender Could Not Solve Some Issues

In most cases BitDefender successfully disinfects the infected files it detects or it isolates the infection. However, there are issues that cannot be solved.



In these cases, we recommend you to contact the BitDefender Support Team at www.bitdefender.com. Our support representatives will help you solve the issues you are experiencing.

BitDefender Detected Suspect Files

Suspect files are files detected by the heuristic analysis as potentially infected with malware the signature of which has not been released yet.

If suspect files were detected during the scan, you will be requested to submit them to the BitDefender Lab. Click **OK** to send these files to the BitDefender Lab for further analysis.

16.2.6. Viewing Scan Logs

To see the scan results after a task has run, right-click the task and select **Logs**. The following window will appear:

Overview	Paths	Scheduler	Logs
Status	Date & Time	Summary	
		Delete	Show
Q			
		04	Canad

Here you can see the report files generated each time the task was executed. For each file you are provided with information on the status of the logged scanning process, the date and time when the scanning was performed and a summary of the scanning results.


Two buttons are available:

- Delete to delete the selected scan log.
- Show to view the selected scan log. The scan log will open in your default web browser.



Note

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.

Scan Log Example

The following figure represents an example of a scan log:



Scan Log Example

The scan log contains detailed information about the logged scanning process, such as scanning options, the scanning target, the threats found and the actions taken on these threats.

16.3. Objects Excluded from Scanning

There are cases when you may need to exclude certain files from scanning. For example, you may want to exclude an EICAR test file from on-access scanning or .avi files from on-demand scanning.



BitDefender allows excluding objects from on-access or on-demand scanning, or from both. This feature is intended to decrease scanning times and to avoid interference with your work.

Two types of objects can be excluded from scanning:

- Paths the file or the folder (including all the objects it contains) indicated by a specified path will be excluded from scanning.
- **Extensions** all files having a specific extension will be excluded from scanning.



Note

The objects excluded from on-access scanning will not be scanned, no matter if they are accessed by you or by an application.

To see and manage the objects excluded from scanning, go to **Antivirus>Exceptions** in the Advanced View.

BitDefender Antivir	us 2009 - Tri	ial			SWITCH TO BASI	C VIEW
STATUS: There are 2 pen	ding issues					FIX ALL ISSUES
	Shield	Virus Scan	Excludes	Quarantine		
General						
Antivirus	Exceptions ar	e enabled				
Privacy Control						
Vulnerability		Excluded obje	ts from scanning		On Access	On Demand
Encryption		Files a	nd folders			
Network						
Update						
Registration						
		Ext	ensions		Apply	Discard
By defining specific exclus	ions, the antivirus mo	dule will except spe	tific files or folders f	rom scanning.		
(Spitdefender)				My Account -	<u>Register</u> - <u>Help</u> -	Support - History
Exceptions						



You can see the objects (files, folders, extensions) that are excluded from scanning. For each object you can see if it is excluded from on-access, on-demand scanning or both.



The exceptions specified here will NOT apply for contextual scanning.

To remove an entry from the table, select it and click the \blacksquare **Delete** button.

To edit an entry from the table, select it and click the \square **Edit** button. A new window will appear where you can change the extension or the path to be excluded and the type of scanning you want them to be excluded from, as needed. Make the necessary changes and click **OK**.



Note

Note

You can also right-click an object and use the options on the shortcut menu to edit or delete it.

You can click **Discard** to revert the changes made to the rule table, provided that you have not saved them by clicking **Apply**.

16.3.1. Excluding Paths from Scanning

To exclude paths from scanning, click the **Add** button. You will be guided through the process of excluding paths from scanning by the configuration wizard that will appear.



Step 1/4 - Select Object Type

Defend	der 2009					-
lusions	Wizard - Step 1 o	f 4				
St	tep 1	Step 2	Step 3		Step 4	
ase choose	e what type of rule yo	u want to create. You car	n choose to exclude path	ns or extensio	ins.	
The I mode you an o	BitDefender Exclusions Wiz ule to except specific files (are an administrator and y n-demand scan of the excl	eard will guide you through the or folders from scanning. It is r ou have previously scanned th uded items to ensure that you	necessary steps to create ru ot recommended to exclude e excluded items. BitDefend r computer is virus free.	iles that will ena files or folders fi er will ask you if	ble the antivirus rom scanning, unle you want to perfe	ess orm
	Do not scan file or l Do not scan extens	folder paths iions				
Please cho sure that y	ose the exceptions for the rour system is fully protect	scanning process carefully an ed	d remember that it is recomm	ended not to de	fine any exception	n in order
oitdefen	der			Back	Next	Cance
ect Tv	pe					

Select the option of excluding a path from scanning.

Step 2/4 - Specify Excluded Paths

lusions Wizard - Step	2 of 4		
Step 1	Step 2	Step 3	Step 4
lude paths	uld not be cranned		
se encernere che paur chac she			Browse Add
ected paths			
documents and settings\vd	anciu\desktop\eicar test\		
Above you can browse	for the path that you want to exclude fro	m scanning. Please make sure that	you click add after you choose
excluded path (rile or r	older). You can add multiple items to this lis	sc.	
Please choose the exceptions f sure that your system is fully p	or the scanning process carefully and reme rotected	ember that it is recommended not to	define any exception in order
itdefender		Back	Next Canc
		Daran	I carre

To specify the paths to be excluded from scanning use either of the following methods:

- Click Browse, select the file or folder that you want to be excluded from scanning and then click Add.
- Type the path that you want to be excluded from scanning in the edit field and click Add.



Note

If the provided path does not exist, an error message will appear. Click **OK** and check the path for validity.

The paths will appear in the table as you add them. You can add as many paths as you want.

To remove an entry from the table, select it and click the \blacksquare **Delete** button.

Step 3/4 - Select Scanning Type

Step 1	Step 2	Step 3	Step 4
In to apply se choose the type of scan that column of the table below and	t will apply to the selected exceptions: or select the option that best suits your nee	-demand, on-access or both. Cli sds.	ck the text in each cell in the
lected objects			When to apply
documents and settings\vd	lanciu\desktop\eicar_test\		On-access
Please choose the exceptions sure that your system is fully p	for the scanning process carefully and re protected	nember that it is recommended r	not to define any exception in orde
#defenden			No. 1

You can see a table containing the paths to be excluded from scanning and the type of scanning they are excluded from.

By default, the selected paths are excluded from both on-access and on-demand scanning. To change when to apply the exception, click on the right column and select the desired option from the list.



Step 4/4 - Scan Excluded Files

Bit Def	ender 2009			_ ×
Exclusio	ons Wizard - Step	9 4 of 4		
Finish	Step 1	Step 2	Step 3	Step 4
	We recommend you to p Please note that if you the wizard you will be re	perform an on-demand task of the exc choose to go on with the scanning tas quested to choose the actions to be t	luded target to make sure that your c , an on-demand scan wizard will be d aken in case viruses are found.	omputer is virus free. isplayed. At the end of
	Select this if you war	nt the scanning task to be started whe	n you click finish	
Pleas	e choose the exceptions f	or the scanning process carefully and	remember that it is recommended not	to define any exception in order to be
(Shitda	that your system is fully pr	rotected		T risk T result
<i>bitde)</i> Scan E	<i>fender</i> xcluded Files	3	Back	Finish Cancel

It is highly recommended to scan the files in the specified paths to make sure that they are not infected. Select the check box to scan these files before excluding them from scanning.

Click Finish.

Click Apply to save the changes.

16.3.2. Excluding Extensions from Scanning

To exclude extensions from scanning, click the Add button. You will be guided through the process of excluding extensions from scanning by the configuration wizard that will appear.



Step 1/4 - Select Object Type

Bit Defender 2009			_ ×
Exclusions Wizard - St	tep 1 of 4		
Step 1	Step 2	Step 3	Step 4
Please choose what type of	f rule you want to create. You can o	choose to exclude paths or ext	ensions.
The BitDefender Excl module to except spe you are an administr an on-demand scan o	usions Wizard will guide you through the ne cific files or folders from scanning. It is not stor and you have previously scanned the f the excluded items to ensure that your c	acessary steps to create rules that wi recommended to exclude files or fol excluded items. BitDefender will ask omputer is virus free.	ill enable the antivirus ders from scanning, unless you if you want to perform
 Do not so Do not so 	an file or folder paths an extensions		
	- 6 - W		
sure that your system is ful	ns for the scanning process carefully and r ly protected	emember that it is recommended not	to define any exception in order to be
Sitdefender		Back	Next Cancel
bject Type			

Select the option of excluding an extension from scanning.



Step 2/4 - Specify Excluded Extensions

clusions Wizard - Step 2 of 4		
Step 1 Step 2	Step 3	Step 4
clude extensions		
sase enter here the extensions that should not be scanned		
Add		
		-
elected extensions		
avi (Audio Video Interleaved animation file)		
Above you can select the extensions that you want to exclu an extension. You can add multiple items to this list.	ude from scanning. Please make sure	that you click add after you choose
Please choose the exceptions for the scanning process carefully and sure that your system is fully protected	d remember that it is recommended n	ot to define any exception in order to

To specify the extensions to be excluded from scanning use either of the following methods:

Select from the menu the extension that you want to be excluded from scanning and then click Add.



Note

The menu contains a list of all the extensions registered on your system. When you select an extension, you can see its description, if available.

Type the extension that you want to be excluded from scanning in the edit field and click Add.

The extensions will appear in the table as you add them. You can add as many extensions as you want.

To remove an entry from the table, select it and click the **Delete** button.



Click Next.

Step 3/4 - Select Scanning Type

Step 1	Step 2	Step 3	Step 4
hen to apply			
ase choose the type of scan that will ht column of the table below and selec	apply to the selected exceptions: (ct the option that best suits your n	on-demand, on-access or both. Click eeds.	< the text in each cell in the
elected objects			When to apply
avi (Audio Video Interleaved ani،	mation file)		Both
Please choose the exceptions for the sure that your system is fully prote	te scanning process carefully and r	emember that it is recommended no	at to define any exception in order
Please choose the exceptions for th sure that your system is fully prote	re scanning process carefully and r cted	remember that it is recommended no	ot to define any exception in orde

You can see a table containing the extensions to be excluded from scanning and the type of scanning they are excluded from.

By default, the selected extensions are excluded from both on-access and on-demand scanning. To change when to apply the exception, click on the right column and select the desired option from the list.



Step 4/4 - Select Scanning Type

<mark>Bit</mark> Def	ender 2009			_ 2
xclusio	ons Wizard - Step 4 (of 4		
	Step 1	Step 2	Step 3	Step 4
Finish				
i	We recommend you to perfo Please note that if you choo the wizard you will be reques	rm an on-demand task of the excl se to go on with the scanning task ted to choose the actions to be t	uded target to make sure that your c , an on-demand scan wizard will be d aken in case viruses are found.	omputer is virus free. isplayed. At the end of
Pleas	e choose the exceptions for th that your system is fully protec	e scanning process carefully and r ted	remember that it is recommended not	to define any exception in order to I
bitde	fender		Back	Finish Cancel
canni	ng Type			

It is highly recommended to scan the files having the specified extensions to make sure that they are not infected.

Click Finish.

Click **Apply** to save the changes.

16.4. Quarantine Area

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.

To see and manage quarantined files and to configure the quarantine settings, go to **Antivirus>Quarantine** in the Advanced View.

BitDefender Antivi	us 2009 - Tri	al			SWITCH TO BASIC	VIEW - ×
STATUS: There are 2 per	ding issues				F	IX ALL ISSUES
	Shield	Virus Scan	Excludes	Quarantine		
General						
Antivirus	Quarantine Fol	ler				
Privacy Control						-
Vulnerability	File na	me	Virus name		Location	Sent
Encryption						
Network						
Update						
Registration						
This is a list of the files th	at were added to the	Quarantine folder d	uring the last scanning	Settings	Send	Restore
(Spitdefender)				My Account	- <u>Register</u> - <u>Help</u> - <u>S</u>	upport - <u>History</u>
Quarantine						

The Quarantine section displays all the files currently isolated in the Quarantine folder. For each quarantined file, you can see its name, the name of the detected virus, the path to its original location and the submission date.



Note

When a virus is in quarantine it cannot do any harm because it cannot be executed or read.

16.4.1. Managing Quarantined Files

To delete a selected file from quarantine, click the \square **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**.



Contextual Menu. A contextual menu is available, allowing you to manage quarantined files easily. The same options as those mentioned previously are available. You can also select **Refresh** to refresh the Quarantine section.

16.4.2. Configuring Quarantine Settings

To configure the quarantine settings, click Settings. A new window will appear.

tDefender - Quarantine Settings		
Delete old files		
Delete files older than	30	day(s)
Check for old files every	1	day(s)
Delete duplicates		
Check for duplicates every	1	day(s)
Automatically submit files		
Submit files every	60	minute(s)
Scan quarantined files after update		
Restore clean files		
Here you can configure the quarantine settings		
OK Cancel		
arantina Sattinga		

Using the quarantine settings, you can set BitDefender to automatically perform the following actions:

Delete old files. To automatically delete old quarantined files, check the corresponding option. You must specify the number of days after which the quarantined files should be deleted and frequency with which BitDefender should check for old files.



Note

By default, BitDefender will check for old files every day and delete files older than 30 days.

Delete duplicates. To automatically delete duplicate quarantined files, check the corresponding option. You must specify the number of days between two consecutive checks for duplicates.





Note

By default, BitDefender will check for duplicate quarantined files every day.

Automatically submit files. To automatically submit quarantined files, check the corresponding option. You must specify the frequency with which to submit files.



Note

By default, BitDefender will automatically submit quarantined files every 60 minutes.

Scan quarantined files after update. To automatically scan quarantined files after each update performed, check the corresponding option. You can choose to automatically move back the cleaned files to their original location by selecting **Restore clean files**.

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



17. Privacy Control

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.

17.1. Privacy Control Status

To configure the Privacy Control and to view information regarding its activity, go to **Privacy Control>Status** in the Advanced View.

BitDefender Antiv	/irus 2009 - Trial	SWITCH TO BASIC VIEW
STATUS: There are 2 p	ending issues	FIX ALL ISSUES
	Status Identity	Registry Cookie Script
General		
Antivirus	Privacy protection is enable	ed
Privacy Control	Identity Control is not configure	ed
Vulnerability	Protection Louel	
Encryption	Protection Level	
Network	- Aggressive	DEFAULT
Update		- Identity control is enabled
Registration	Default	- Registry control is enabled - Cookie control is disabled - Script control is disabled
	- Permissive	
		<u>Eustom Level</u> Default Level
	Privacy Control Statistics	
	Identity information blocked: Registry blocked: Cookies blocked: Scripts blocked:	0 0 0 0
Q		
(Spitdefender)		<u>My Account</u> - <u>Register</u> - <u>Help</u> - <u>Support</u> - <u>History</u>
Privacy Control	Status	

You can see whether Privacy Control is enabled or disabled. If you want to change the Privacy Control status, clear or select the corresponding check box.





Important

To prevent data theft and protect your privacy keep the **Privacy Control** enabled.

The Privacy Control protects your computer using these important protection controls:

- Identity Control protects your confidential data by filtering all outgoing web (HTTP), e-mail (SMTP) and instant messaging traffic according to the rules you create in the Identity 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.
- 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.

At the bottom of the section you can see the Privacy Control statistics.

17.1.1. Configuring 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 Identity Control are enabled.
Aggressive	Registry control, Identity Control and Script Control are enabled.

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

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



17.2. Identity Control

Keeping confidential data safe is an important issue that bothers us all. Data theft has kept pace with the development of Internet communications and it makes use of new methods of fooling people into giving away private information.

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.

Identity Control protects you against the theft of sensitive data when you are online. Based on the rules you create, Identity Control scans the web, e-mail and instant messaging traffic leaving your computer for specific character strings (for example, your credit card number). If there is a match, the respective web page, e-mail or instant message is blocked.

You can create rules to protect any piece of information you might consider personal or confidential, from your phone number or e-mail address to your bank account information. Multiuser support is provided so that users logging on to different Windows user accounts can configure and use their own identity protection rules. The rules you create are applied and can be accessed only when you are logged on to your Windows user account.

Why you use Identity Control?

Identity Control is very effective in blocking keylogger spyware. This type of malicious applications records your keystrokes and sends them over the Internet to a malicious person (hacker). The hacker can find out sensitive information from the stolen data, such as bank account numbers and passwords, and use it to gain personal benefits.

Supposing such an application manages to avoid antivirus detection, it cannot send the stolen data by e-mail, web or instant messages if you have created appropriate identity protection rules.

Identity Control can protect you from phishing attempts (attempts to steal personal information). The most common phishing attempts make use of a deceiving e-mail to trick you into submitting personal information on a fake web page.

For example, you may receive an e-mail claiming to be from your bank and requesting you to urgently update your bank account information. The e-mail provides you with a link to the web page where you must provide your personal information. Although they seem to be legitimate, the e-mail and the web page the misleading link directs you to are fake. If you click the link in the e-mail and submit your personal



information on the fake web page, you will disclose this information to the malicious persons who organized the phishing attempt.

If appropriate identity protection rules are in place, you cannot submit personal information (such as your credit card number) on a web page unless you have explicitly defined an exception for the respective web page.

To configure Identity Control, go to **Privacy Control>Identity** in the Advanced View.

BitDefender Antivirus 2009 - Trial SWITCH TO BASIC VIEW									
STATUS: There are 2 pe	ending issues								FIX ALL ISSUES
	Status	Ide	ntity		Rej	gistry	Cookie	Script	
General									
Antivirus	🖌 Identity p	rotection							
Privacy Control	Total attem	pts blocked:	0						• - •
Vulnerability	Rule Name	Rule Type	н	Smtp	IM	Whole words	Match case	Description	
Encryption									
Network									
Update									
Registration									
									Exceptions
List of user defined ider	itity rules. You can	change this lis	t by cl	icking o	n add,	, edit or remove	buttons	<u>Register</u> - <u>Hel</u> r	2 - <u>Support</u> - <u>History</u>

If you want to use Identity Control, follow these steps:

- 1. Select the **Identity Control** check box.
- 2. Create rules to protect your sensitive data. For more information, please refer to "Creating Identity Rules" (p. 148).
- 3. If needed, define specific exceptions to the rules you have created. For more information, please refer to "*Defining Exceptions*" (p. 151).



17.2.1. Creating Identity Rules

To create an identity protection rule, click the \blacksquare Add button and follow the configuration wizard.

Step 1/4 - Welcome Window





Step 2/4 - Set Rule Type and Data

BitDefender W	izard
Rule Name	dfdfd
Rule Type	address
Rule Data Personal info but you. For you would lik address: johr target string.	mnkl mation is encrypted and it cannot be used by anyone else extra safety, please enter just part of the information that to protect (e.g., if you want to filter traffic for this e-mail obeelexample.com, you should only include "john" in the
Q	
	Next > Cancel
Set Rule Type	and Data

You must set the following parameters:

- **Rule Name** type the name of the rule in this edit field.
- **Rule Type** choose the rule type (address, name, credit card, PIN, SSN etc).
- **Rule Data** type the data you want to protect in this edit field. For example, if you want to protect your credit card number, type all or part of it here.



Note

If you enter less than three characters, you will be prompted to validate the data. We recommend you to enter at least three characters in order to avoid the mistaken blocking of messages and web pages.

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



Step 3/4 - Select Traffic

BitDefender Wizard
Scan Http
🖌 Scan Smtp
Scan Instant Messaging
Match whole words
Match case
Http (web) traffic and sntp (e-mail) traffic containing your personal information will be blocked.
0
Next > Cancel
Select Traffic

Select the type of 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.
- **Scan Instant Messaging** scans the Instant Messaging traffic and blocks the outgoing chat messages that contain the rule data.

You can choose to apply the rule only if the rule data matches whole words or if the rule data and the detected string case match.



Step 4/4 - Describe Rule

BitDefender Wizard		
Rule Description		
Jhidybido		
Enter a description for this rule. The description should h administrators identify what information you blocked wit	help you or other h more ease.	
Q		
	Finish	Cancel
Describe Rule		

Enter a short description of the rule in the edit field. Since the blocked data (character string) is not displayed in plain text when accessing the rule, the description should help you easily identify it.

Click **Finish**. The rule will appear in the table.

17.2.2. Defining Exceptions

There are cases when you need to define exceptions to specific identity rules. Let's consider the case when you create a rule that prevents your credit card number from being sent over HTTP (web). Whenever your credit card number is submitted on a website from your user account, the respective page is blocked. If you want, for example, to buy footwear from an online shop (which you know to be secure), you will have to specify an exception to the respective rule.

To open the window where you can manage exceptions, click **Exceptions**.



All and a state in the second state in a	E time to	
Allowed Web/e-mail address	Exception ty	pe
	Add	Remove
	OK	Cancel

To add an exception, follow these steps:

- 1. Click **Add** to add a new entry in the table.
- 2. Double-click **Specify allowed address** and provide the web site, the e-mail address or the IM contact that you want to add as exception.
- 3. Double-click **Choose type** and choose from the menu the option corresponding to the type of address previously provided.
 - If you have specified a web address, select HTTP.
 - If you have specified an e-mail address, select SMTP.
 - If you have specified an IM contact, select IM.

To remove an exception from the list, select it and click **Remove**.

Click **OK** to save the changes.

17.2.3. Managing Rules

You can see the rules created so far listed in the table.

To delete a rule, select it and click the **Delete** button.



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

Rule Name	dfdfd
Rule Type	address 💌
Rule data	•••••
🖌 Scan Http	Match whole words
🖌 Scan Smtp	Match case
🖌 Scan IM	
Rule description	
jhkhjbkb	
Q	
	OK Cancel

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

17.3. Registry Control

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

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

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



BitDefender Registry Alert				
	Hicrosoft® Windows® Operating is trying to modify Windows Registry			
	Registry key: C:\\Program Files			
Q	If you recognize this program, we recommend you to allow this action.			
	Allow Block			

Registry Alert

You can see the program that is trying to modify Windows Registry.

If you do not recognize the program and if it seems suspicious, click **Block** to prevent it from modifying Windows Registry. Otherwise, click **Allow** to permit the modification.

Based on your answer, a rule is created and listed in the rules table. The same action is applied whenever this program tries to modify a registry entry.



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

To configure Registry Control, go to Privacy Control>Registry in the Advanced View.

BitDefender Antivirus 2009 - Trial SWITCH TO BASIC VIEW						
STATUS: There are 2 pen	ding issues				FI	X ALL ISSUES
	Status Iden	ity	Registry	Cookie	Script	
General						
Antivirus	Enable Registry Contro	I				
Privacy Control	Total attempts blocked:	0				
Vulnerability	Name	Action	Application pat	h		
Encryption	Messenger	Permit	E:\Program File	is\Messenger\msms	gs.exe	
Network						
Update						
Registration						
List with Registry Control	rules enabled on your computer.	You can ch	nange this list by (dicking on remove l	outton	
(Spitdefender)				My Account	<u>Register</u> - <u>Help</u> - <u>Su</u>	pport - History
Registry Control						

You can see the rules created so far listed in the table.

To delete a rule, select it and click the \blacksquare **Delete** button.

17.4. Cookie Control

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

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

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



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



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.

To configure Cookie Control, go to Privacy Control>Cookie in the Advanced View.

STATUS: There are 2 p	ending issues			FIX ALL ISSUES
	Status Identity	Registry Coo	kie Script	
ieneral				
ntivirus	Enable Cookie Control			
rivacy Control	Total cookies blocked: 0			
ulnerability	Domain	Direction	Action	
ncryption				
etwork				
pdate				
egistration				
List with cookies enab	led on your web browser. You can chang	ge this list by clicking on add or remo	ove buttons.	
Shitdefenden		My Ar	count - Register - Help -	Support - History

You can see the rules created so far listed in the table.



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, select it and click the **Delete** button. To modify the rule parameters, double-click the rule and make the desired changes in the configuration window.

To manually add a rule, click the Add button and configure the rule parameters in the configuration window.

17.4.1. Configuration Window

When you edit or manually add a rule, the configuration window will appear.



Select Address, Action and Direction
Enter domain Any Enter domain Fields action Permit Deny Select direction Outgoing Dutoping 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.
Q
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.

Туре	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.





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

Click Finish.

17.5. Script Control

Note

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.

To configure Script Control, go to Privacy Control>Script in the Advanced View.

BitDefender Antivi	irus 2009 - Tria	ıl			SWITCH TO BAS	C VIEW 📃 🗵
STATUS: There are 2 pe	nding issues					FIX ALL ISSUES
	Status	Identity	Registry	Cookie	Script	
General						
Antivirus	Enable Script Control					
Privacy Control	l otal scripts block	ed: U				
Vulnerability	Domain			Action		
Encryption						
Network						
Update						
Registration						
Q						
(Spitdefender				My Account -	<u>Register</u> - <u>Help</u> -	Support - History
Script Control						

You can see the rules created so far listed in the table.



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, select it and click the **Delete** button. To modify the rule parameters, double-click the rule and make the desired changes in the configuration window.

To manually create a rule, click the Add button and configure the rule parameters in the configuration window.

17.5.1. Configuration Window

When you edit or manually add a rule, the configuration window will appear.



Enter	' domain	
Select	t action	
	 Permit Deny 	
1	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.	

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.



18. Instant Messaging (IM) Encryption

By default, BitDefender encrypts all your instant messaging chat sessions provided that:

- Your chat partner has a BitDefender version installed that supports IM Encryption and IM Encryption is enabled for the instant messaging application used for chatting.
- You and your chat partner use either Yahoo Messenger or Windows Live (MSN) Messenger.



Important

BitDefender will not encrypt a conversation if a chat partner uses a web-based chat application, such as Meebo, or other chat application that supports Yahoo Messenger or MSN.

To configure instant messaging encryption, go to **Encryption>IM Encryption** in the Advanced View.



Note

You can easily configure instant messaging encryption using the BitDefender toolbar from the chat window. For more information, please refer to "*Integration into Messenger*" (p. 34).

BitDefender Antivirus 2009 - Trial			SWITCH TO BASIC VIEW		
STATUS: There is 1 pe	ending issue		FIX ALL ISSUES		
	IM Encryption				
General					
Antivirus	✓ IM Encryption is e	enabled.			
Privacy Control	✓ Yahoo Messeng	er Encryption is enabled.			
Vulnerability	Windows Live (MSN) Messenger Encryption is enabled.				
Encryption	Encryption Exclusion	ons			
Game/Laptop Mode					
Network	User ID		IM Program		
Update					
Registration					
	Current Connection	ns			
	User ID	IM Program	Encryption Status		
Rease click the 'FIX A	ALL ISSUES' button to see the o	letailed list of issues that affect your	system's security.		
(Spitdefender)		Bu	y - <u>My Account</u> - <u>Register</u> - <u>Help</u> - <u>Support</u> - <u>History</u>		
notont Maaaaa	ning Enoruption				

Instant Messaging Encryption

By default, IM Encryption is enabled for both Yahoo Messenger and Windows Live (MSN) Messenger. You can choose to disable IM Encryption for a specific chat application only or completely.

Two tables are displayed:

- Encryption Exclusions lists the user IDs and the associated IM program for which encryption is disabled. To remove a contact from the list, select it and click the Remove button.
- Current Connections lists the current instant messaging connections (user ID and associated IM program) and whether or not they are encrypted. A connection may not be encrypted for these reasons:
 - · You explicitly disabled encryption for the respective contact.
 - Your contact does not have installed a BitDefender version that supports IM encryption.



18.1. Disabling Encryption for Specific Users

To disable encryption for a specific user, follow these steps:

1. Click the **Add** button to open the configuration window.

itDefender - 1	Instant Messaging user setting3
User ID	
IM Program	 Yahoo Messenger Windows Live (MSN) Messenger
	OK Cancel

- 2. Type in the edit field the user ID of your contact.
- 3. Select the instant messaging application associated with the contact.
- 4. Click OK.



19. Vulnerability

An important step in protecting your computer against malicious persons and applications is to keep up to date the operating system and the applications you regularly use. Moreover, to prevent unauthorized physical access to your computer, strong passwords (passwords that cannot be easily guessed) must be configured for each Windows user account.

BitDefender regularly checks your system for vulnerabilities and notifies you about the existing issues.

19.1. Status

To configure the automatic vulnerability checking or run a vulnerability check, go to **Vulnerability>Status** in the Advanced View.

BitDefender Antivir	us 2009 - Trial	SWITCH TO BASIC VIEW
STATUS: There are 2 pen	ding issues	FIX ALL ISSUES
	Status Settings	
General		
Antivirus	✓ Automatic ¥ulnerability Checking is enabled	
Privacy Control		Check Now
Vulnerability		
Encryption	Last Yulnerability Check Status	
Network		
Update		
Registration		
Q		
(Spitdefender)		<u>My Account</u> - <u>Register</u> - <u>Help</u> - <u>Support</u> - <u>History</u>
Vulnerability Stat	tus	


The table displays the issues covered in the last vulnerability check and their status. You can see the action you have to take to fix each vulnerability, if any. If the action is **None**, then the respective issue does not represent a vulnerability.



Important

To be automatically notified about system or application vulnerabilities, keep the **Automatic Vulnerability Checking** enabled.

19.1.1. Fixing Vulnerabilities

To fix a specific vulnerability, double click it and, depending on the issue, proceed as follows:

- If Windows updates are available, click Install All System Updates to install them.
- If an application is outdated, use the Home Page link provided to download and install the latest version of that application.
- If a Windows user account has a weak password, force the user to change the password at the next logon or change the password yourself.

You can click **Check Now** and follow the wizard to fix vulnerabilities step by step.



Step 1/6 - Select Vulnerabilities to Check

Bit Defender An	tivirus 2009				_ ×
Vulnerability Scan					
Step 1 - Select tasks	Step 2 - Scanning	Step 3 - Passwords	Step 4 - Applications	Step 5 - Windows	Step 6 - Finish
Select tasks					
The wizard searches for ava applications that are checke select all the boxes below.	ilable Windows updates, d for these vulnerabilities	weak passwords to Win . In order for all of these	dows accounts and outdate e applications to be fully up	d applications. BitDefender o dated and protected, it is re-	contains a list of commended to
User Passwords					
 Applications Updates 					
Critical Windows Upda	tes				
Other Windows Updat	es				
Select the actions the	e vulnerability module sho	uld take when checking	your system.		
νĩ					
(Spitdefender)					Next Cancel
/ulnerabilities					

Click Next to check the system for the selected vulnerabilities.



Step 2/6 - Checking for Vulnerabilities

Bit Defender A	ntivirus 2009				_ ×
Vulnerability Scan					
Step 1 - Select tasks	Step 2 - Scanning	Step 3 - Passwords	Step 4 - Applications	Step 5 - Windows	Step 6 - Finish
Status					
Scanning	🐛 Critical Windows	Updates			
	re le la prograde				
C The scaling proces	is is in progress				
(Spitdefender)					Stop Cancel
Vulnerability C	heck				

Wait for BitDefender to finish checking for vulnerabilities.



Step 3/6 - Change Weak Passwords

Julnerability Scan					
Step 1 - Select tasks	Step 2 - Scanning	Step 3 - Passwords	Step 4 - Applications	Step 5 - Windows	Step 6 - Finis
lser Passwords					
User Name	Strengt	th Statu	s		
Administrator	Strong	Ok			2
cosmin	Weak	Fix			
This is a list of the W	indows accounts password	ds set on your computer a	and the level of protection t	hat they provide. Click the	'Fix' button to more

You can see the list of the Windows user accounts configured on your computer and the level of protection their password provides.

Click Fix to modify the weak passwords. A new window will appear.

BitDefender
Choose method to fix:
 Force user to change password at next login Change user password
Type password:
Confirm password:
OK Clase
Change Password



Select the method to fix this issue:

- Force user to change password at next login. BitDefender will prompt the user to change the password the next time the user logs on to Windows.
- Change user password. You must type the new password in the edit fields.



Note

For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, \$ or @).

Click **OK** to change the password.

Click Next.

Step 4/6 - Update Applications

Bit Defender Ant	tivirus 2009				-	×
Vulnerability Scan						
Step 1 - Select tasks	Step 2 - Scanning	Step 3 - Passwords	Step 4 - Applications	Step 5 - Windows	Step 6	- Finish
Applications Updates						
Application Name		I	nstalled Version	Latest Version	Download	
Yahoo! Messenger			8.1.0.421	8.1.0.241	Up To Date	
Winamp			5,5,3,1938	5,5,3,1924	Up To Date	
Firefox			2.0.0.15 (en-US)	3.0 (en-US)	Home Page	
						Y
C This is a list of the app	lications supported by B	itDefender and of the up	dates available, if any.			
(Spitdefender)					Next C	ancel
Applications						

You can see the list of applications checked by BitDefender and if they are up to date. If an application is not up to date, click the provided link to download the latest version.



Click Next.

Step 5/6 - Update Windows

					Vulnerability Scan
Step 6 - Finis	Step 5 - Windows	Step 4 - Applications	Step 3 - Passwords	Step 2 - Scanning	Step 1 - Select tasks
					Windows Updates
4				ates	Critical Windows Upd
		31)) Service Pack 2 (KB93618	oft XML Core Services 4.0	Security Update for Microso
				tes	Other Windows Upda
				category	No updates available in this
				tes	Install All System Upda
2			applications updates	tes	Install All System Upda

You can see the list of critical and non-critical Windows updates that are not currently installed on your computer. Click **Install All System Updates** to install all the available updates.

Click Next.



Step 6/6 - View Results

it Defender An	tivirus 2009				
ulnerability Scan					
Step 1 - Select tasks	Step 2 - Scanning	Step 3 - Passwords	Step 4 - Applications	Step 5 - Windows	Step 6 - Fin
The vulnerability	scan is finished. 1	ïhe tasks you selec	ted at Step 1 have b	een performed.	
The vulnerability scan	is finished. The tasks y	ou selected at Step 1 have	e been performed.		
bitdefender					flos

Click Close.

19.2. Settings

To configure the settings of the automatic vulnerability checking, go to **Vulnerability>Settings** in the Advanced View.

BitDefender Antivi	rus 2009 - Trial	SWITCH TO BASIC VIEW
STATUS: There are 2 per	nding issues	FIX ALL ISSUES
	Status Settings	
General		
Antivirus	Yulpershilities to be checked	
Privacy Control		
Vulnerability	 Critical Windows Updates 	
Encryption	Regular Windows Updates	
Network	✓ Weak Passwords	
Update		
Registration	Application Updates	
Q		
(Bitdefender)		My Account - Register - Help - Support - History
Automotio Vulno	rability Chaoking Sattings	

Automatic Vulnerability Checking Settings

Select the check boxes corresponding to the system vulnerabilities you want to be regularly checked.

- Critical Windows Updates
- Regular Windows Updates
- Weak Passwords
- Applications Updates



Note

If you clear the check box corresponding to a specific vulnerability, BitDefender will no longer notify you about the related issues.



20. Game / Laptop Mode

The Game / Laptop Mode module allows you to configure the special operation modes of BitDefender:

- Game Mode temporarily modifies the product settings so as to minimize the resource consumption when you play.
- Laptop Mode prevents scheduled tasks from running when the laptop is running on battery in order to save battery power.

20.1. Game Mode

Game Mode temporarily modifies protection settings so as to minimize their impact on system performance. While in Game Mode, the following settings are applied:

- All BitDefender alerts and pop-ups are disabled.
- The BitDefender real-time protection level is set to **Permissive**.
- Updates are not performed by default.



Note

To change this setting, go to Update>Settings and clear the Don't update if Game Mode is on check box.

Scheduled scan tasks are by default disabled.

By default, BitDefender automatically enters Game Mode when you start a game from the BitDefender's list of known games or when an application goes to full screen. You can manually enter Game Mode using the default Ctrl+Alt+Shift+G hotkey. It is strongly recommended that you exit Game Mode when you finished playing (you can use the same default Ctrl+Alt+Shift+G hotkey).



Note

While in Game Mode, you can see the letter G over the **@** BitDefender icon.

To configure Game Mode, go to **Game / Laptop Mode>Game Mode** in the Advanced View.



At the top of the section, you can see the status of the Game Mode. You can click **Enter Game Mode** or **Exit Game Mode** to change the current status.

20.1.1. Configuring Automatic Game Mode

Automatic Game Mode allows BitDefender to automatically enter Game Mode when a game is detected. You can configure the following options:

- Use the default list of games provided by BitDefender to automatically enter Game Mode when you start a game from the BitDefender's list of known games. To view this list, click Manage Games and then View Allowed Games.
- Enter game mode when in full screen to automatically enter Game Mode when an application goes to full screen.



Add the application to the game list? - to be prompted to add a new application to the game list when you leave full screen. By adding a new application to the game list, the next time you start it BitDefender will automatically enter Game Mode.



Note

If you do not want BitDefender to automatically enter Game Mode, clear the **Automatic Game Mode** check box.

20.1.2. Managing the Game List

BitDefender automatically enters Game Mode when you start an application from the game list. To view and manage the game list, click **Manage Games**. A new window will appear.

1y gan	nes list
х	Name
~	game.exe
	View Allowed Games
	his is where you can find a list of applications for which you have set the default Gam Node behaviour.
	OK

New applications are automatically added to the list when:

- You start a game from the BitDefender's list of known games. To view this list, click **View Allowed Games**.
- After leaving full screen, you add the application to the game list from the prompt window.



If you want to disable Automatic Game Mode for a specific application from the list, clear its corresponding check box. You should disable Automatic Game Mode for regular applications that go to full screen, such as web browsers and movie players.

To manage the game list, you can use the buttons placed at the top of the table:

- **Add** add a new application to the game list.
- **Remove** remove an application from the game list.
- **Edit** edit an existing entry in the game list.

Adding or Editing Games

When you add or edit an entry from the game list, the following window will appear:

BitDefender - Game Mode Rules	×
Select application path	
e:\gamelexe Browse	
Enabled	
O Disabled	
Rere is where you can add a new game to the game list already defined.	
OK Cancel	
Add Game	

Click **Browse** to select the application or type the full path to the application in the edit field.

If you do not want to automatically enter Game Mode when the selected application is started, select **Disable**.

Click **OK** to add the entry to the game list.

20.1.3. Configuring Game Mode Settings

To configure the behaviour on scheduled tasks, use these options:

Scan Task - to prevent scheduled scan tasks from running while in Game Mode. You can choose one of the following options:



Option	Description
Skip Task	Do not run the scheduled task at all.
Postpone Task	Run the scheduled task immediately after you exit Game Mode.

20.1.4. Changing Game Mode Hotkey

You can manually enter Game Mode using the default Ctrl+Alt+Shift+G hotkey. If you want to change the hotkey, follow these steps:

1. Click Advanced Settings. A new window will appear.

BitDefender - Advanced Settings	×
✔Use Hotkeys ✔Ctrl ✔Alt ✔Shift G Do not use firewall	
ОК	
Advanced Settings	

- 2. Under the Use HotKey option, set the desired hotkey:
 - Choose the modifier keys you want to use by checking one the following: Control key (Ctrl), Shift key (Shift) or Alternate key (Alt).
 - In the edit field, type the letter corresponding to the regular key you want to use.

For example, if you want to use the Ctrl+Alt+D hotkey, you must check only Ctrl and Alt and type D.

3. Click **OK** to save the changes.



Note

Removing the check mark next to Use HotKey will disable the hotkey.



20.2. Laptop Mode

Laptop Mode is especially designed for laptop and notebook users. Its purpose is to minimize BitDefender's impact on power consumption while these devices are running on battery.

While in Laptop Mode, scheduled tasks are by default not performed.

BitDefender detects when your laptop has switched to battery power and it automatically enters Laptop Mode. Likewise, BitDefender automatically exits Laptop Mode, when it detects the laptop is no longer running on battery.

To configure Laptop Mode, go to **Game / Laptop Mode>Laptop Mode** in the Advanced View.

BitDefender Antivir	us 2009 - Trial	SWITCH TO BASIC VIEW
STATUS: There is 1 pend	ing issue	FIX ALL ISSUES
	Game Mode Laptop Mode	
General		
Antivirus	 Laptop Mode is enabled 	
Privacy Control	🖌 Scan Task	
Vulnerability	Skip Task	
Encryption	Postpone	
Game/Laptop Mode		
Network		
Update		
Registration		
C This is where you can con	figure in detail the Laptop Mode.	
(Spitdefender)		Buy - My Account - Register - Help - Support - History
Laptop Mode		

You can see whether Laptop Mode is enabled or not. If Laptop Mode is enabled, BitDefender will apply the configured settings while the laptop is running on battery.



20.2.1. Configuring Laptop Mode Settings

To configure the behaviour on scheduled tasks, use these options:

Scan Task - to prevent scheduled scan tasks from running while in Laptop Mode. You can choose one of the following options:

Option	Description
Skip Task	Do not run the scheduled task at all.
Postpone Task	Run the scheduled task immediately after you exit Laptop Mode.



21. Network

The Network module allows you to manage the BitDefender products installed on your home computers from a single computer.

BitDefender Antivir	us 2009 - Trial	SWITCH TO BASIC VIEW
STATUS: There are 2 pen	ding issues	FIX ALL ISSUES
	Network	
General		
Antivirus	INTERNET	
Privacy Control		•
Vulnerability		
Encryption	empty	empty
Network		
Update	empty	empty
Registration		
	enply	Join/Create Network
Click Join/Create to start o	reating your nome network	
(Spitdefender)		My Account - Register - Help - Support - History
Network Map		

To be able to manage the BitDefender products installed on your home computers, you must follow these steps:

- 1. Join the BitDefender home network on your computer. Joining the network consists in configuring an administrative password for the home network management.
- 2. Go to each computer you want to manage and join the network (set the password).
- 3. Go back to your computer and add the computers you want to manage.



21.1. Joining the BitDefender Network

To join the BitDefender home network, follow these steps:

1. Click **Join/Create network**. You will be prompted to configure the home management password.

itDefender	x
Enter the home manag	ement password
The password should be at	least 8 characters long
Enter nacculord	
checi passwora.	

Configure Password

- 2. Type the same password in each of the edit fields.
- 3. Click OK.

You can see the computer name appearing in the network map.

21.2. Adding Computers to the BitDefender Network

Before you can add a computer to the BitDefender home network, you must configure the BitDefender home management password on the respective computer.

To add a computer to the BitDefender home network, follow these steps:

1. Click **Manage Network**. You will be prompted to provide the local home management password.



Bit Defender	SitDefender				
You must ente	the home management password.				
Password:	•••••				
Don't show th	Don't show this message again this session.				
	OK Cancel				
Enter Passy	nter Password				

2. Type the home management password and click **OK**. A new window will appear.

BitDefender 🕑
Computer
scohen 📃
scripts2
🐖 sdediu
sgheorghe
sgheorghe2
🛒 sorel 💼
🛒 sqb01 🗸
IP (or hostname) 10.10.13.59
Please select the computers that you want to add to your network.
Add Cancel
dd Computer

You can see the list of computers in the network. The icon meaning is as follows:

- 🗐 Indicates an online computer with no BitDefender products installed.
- Indicates an online computer with BitDefender installed.
- Indicates an offline computer with BitDefender installed.
- 3. Do one of the following:



- Select from the list the name of the computer to add.
- Type the IP address or the name of the computer to add in the corresponding field.
- 4. Click **Add**. You will be prompted to enter the home management password of the respective computer.

itDefender								x
Enter Remote HM Pa	swoi	rd						
The password should be	at lea	st 8 (hara	acte	rs lon	g		
Enter Remote Password		Γ					 	٦
(к				Canc	el		

- 5. Type the home management password configured on the respective computer.
- 6. Click **OK**. If you have provided the correct password, the selected computer name will appear in the network map.



Note

You can add up to five computers to the network map.

21.3. Managing the BitDefender Network

Once you have successfully created a BitDefender home network, you can manage all BitDefender products from a single computer.

ng issue	FIX ALL ISSUES
Network	
INTERNET	
	BDENTLAP5-XP 10.10.15.29
No gatew	1 issues ray found! Trial
BDENTLAP YO	All DC (click to add)
This Comp Register this computer (with a Set the settings password	a license key)
No PC (clic Run a Scan task	(click to add)
Fix issues on this computer	
No PC (cle No no Lipdate on this computer Apply Profile Run a Tuneup task on this co Set this computer as Update	dick to add) mputer Server of this Network Add Computer Leave Network Refresh
puter in your home network. To add a PC you have to j	ioin or create a network by clicking on "Join/Create Network".
	Network

If you move the mouse cursor over a computer from the network map, you can see brief information about it (name, IP address, number of issues affecting the system security, BitDefender registration status).

If you right-click a computer name in the network map, you can see all the administrative tasks you can run on the remote computer.

- Register this computer
- Set the settings password
- Run a scan task
- Fix issues on this computer
- Show history of this computer
- Run an update on this computer now
- Apply profile



- Run a Tuneup task on this computer
- Set this computer as Update Server of this Network

Before running a task on a specific computer, you will be prompted to provide the local home management password.

ient password.
ssion.
Cancel

Type the home management password and click **OK**.



Note

If you plan to run several tasks, you might want to select **Don't show this message again this session**. By selecting this option, you will not be prompted again for this password during the current session.



22. Update

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.

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

If an update is detected, you may be asked to confirm the update or the update is performed automatically, depending on the automatic update settings.

The update process is performed on the fly, meaning that the files to be updated are replaced progressively. In this way, the update process will not affect product operation and, at the same time, any vulnerability will be excluded.

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 antispyware engines new spyware signatures will be added to the database. This update type is also known as Antispyware Update.
- Product upgrades when a new product version is released, new features and scan techniques are introduced to the effect of improving the product's performance. This update type is also known as Product Update.

22.1. Automatic Update

To see update-related information and perform automatic updates, go to **Update>Update** in the Advanced View.

BitDefender Antiv	virus 2009 - Trial		SWITCH TO BASIC VIEW 📃 🕨
STATUS: There are 2 p	ending issues		FIX ALL ISSUES
	Update Se	ttings	
General			
Antivirus	✓ Automatic update is	enabled	
Privacy Control	Last checked	7/17/2008 5:08:15 PM	Undate Now
Vulnerability	Last updated	7/17/2008 5:08:17 PM	opulate non
Encryption			
Network	Antivirus Signature	Properties	
Update	Engine Version	7.20043	Show Virus List
Registration			
	File:	0%	0 kb
	Total update	0 %	0 kb
Q			
Ebitdefender		My Account	<u>t</u> - <u>Register</u> - <u>Help</u> - <u>Support</u> - <u>History</u>
Automatic Unda	ate		

Here you can see when the last check for updates and the last update were performed, as well as information about the last update performed (if successful or the errors that occurred). Also, information about the current engine version and the number of signatures is displayed.

If you open this section during an update, you can see the download status.



Important

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

You can get the malware signatures of your BitDefender by clicking **Show Virus List**. An HTML file that contains all the available signatures will be created and opened in a web browser. You can search through the database for a specific malware signature or click **BitDefender Virus List** to go to the online BitDefender signature database.



22.1.1. Requesting an Update

The automatic update can 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 is recommended to regularly update BitDefender by user request.

22.1.2. Disabling Automatic Update

If you want to disable automatic update, a warning window will appear.

🚦 Th	s option will d	isable the Au	itomatic L	lpdate.
=or how la	ng do you want	to disable the	Automatic L	lpdate?
	5 r	ninutes		•
		0	<	Cancel

Disable Automatic Update

You must confirm your choice by selecting from the menu how long you want the automatic update to be disabled. You can disable the automatic update for 5, 15 or 30 minutes, for an hour, permanently or until the system restart.



Warning

This is a critical security issue. We recommend you to disable automatic update for as little time as possible. If BitDefender is not updated regularly, it will not be able to protect you against the latest threats.



22.2. Update Settings

The updates can be performed from the local network, over the Internet, directly or through a proxy server. By default, BitDefender will check for updates every hour, over the Internet, and install the available updates without alerting you.

To configure the update settings and manage proxies, go to **Update>Settings** in the Advanced View.

BitDefender Antiviru	IS 2009 - Trial SWITCH TO BASIC VIEW
STATUS: There are 2 pend	ing issues FIX ALL ISSUES
	Update Settings
General	Undate Location Fettings
Antivirus	Primary undate location settings
Privacy Control	http://upgrade.bitdefender.com/
Vulnerability	Alternate update location settings
Encryption	http://upgrade.bitdefender.com/
Network	Automatic undate settings
Update	Time interval 1 hours
Registration	Confirm update Silent update Prompt before downloading updates Prompt before installing updates Manual Update Settings Silent update Prompt before downloading updates Advanced settings Wak for reboot, instead of prompting Don't update if Same Mode is on Apply Default Manage proxies
Q	
(Spitdefender)	My Account - Register - Help - Support - History
Update Settings	

The update settings are grouped into 4 categories (**Update Location Settings**, **Automatic Update Settings**, **Manual Update Settings** and **Advanced Settings**). Each category will be described separately.



22.2.1. Setting Update Locations

To set the update locations, use the options from the **Update Location Settings** category.



Note

Configure these settings only if you are connected to a local network that stores BitDefender malware signatures locally or if you connect to the Internet through a proxy server.

For more reliable and faster updates, you can configure two update locations: a **Primary update location** and an **Alternate update location**. By default, these **locations are the same**: http://upgrade.bitdefender.com.

To modify one of the update locations, provide the URL of the local mirror in the **URL** field corresponding to the location you want to change.



Note

We recommend you to set as primary update location the local mirror and to leave the alternate update location unchanged, as a fail-safe plan in case the local mirror becomes unavailable.

In case the company uses a proxy server to connect to the Internet, check **Use proxy** and then click **Manage proxies** to configure the proxy settings. For more information, please refer to "*Managing Proxies*" (p. 192)

22.2.2. Configuring Automatic Update

To configure the update process performed automatically by BitDefender, use the options in the **Automatic Update Settings** category.

You can specify the number of hours between two consecutive checks for updates in the **Time interval** field. By default, the update time interval is set to 1 hour.

To specify how the automatic update process should be performed, select one of the following options:

- Silent update BitDefender automatically downloads and implements the update.
- Prompt before downloading updates every time an update is available, you will be prompted before downloading it.
- Prompt before installing updates every time an update was downloaded, you will be prompted before installing it.



22.2.3. Configuring Manual Update

To specify how the manual update (update by user request) should be performed, select one of the following options in the **Manual Update Settings** category:

- Silent update the manual update will be performed automatically in the background, without user intervention.
- Prompt before downloading updates every time an update is available, you will be prompted before downloading it.

22.2.4. Configuring Advanced Settings

To prevent the BitDefender update process from interfering with your work, configure the options in the **Advanced Settings** category:

- 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.

Don't update if game mode is on - BitDefender will not update if the game mode is turned on. In this way, you can minimize the product's influence on system performance during games.

22.2.5. Managing Proxies

If your company uses a proxy server to connect to the Internet, you must specify the proxy settings in order for BitDefender to update itself. Otherwise, it will use the proxy settings of the administrator that installed the product or of the current user's default browser, if any.



Note

The proxy settings can be configured only by users with administrative rights on the computer or by power users (users who know the password to the product settings).



To manage the proxy settings, click **Manage proxies**. The **Proxy Manager** window will appear.

roxy Settings		
Administrator proxy settings (detected	l at install time)	
Address :	Port :	Username :
		Password :
Current user proxy settings (from defa	ult browser)	
Address :	Port :	Username :
		Password :
Specify your own proxy settings		
Address :	Port :	Username :
		Password :
Q		
		OK Cancel
oxy Manager		

There are three sets of proxy settings:

- Administrator proxy settings (detected at install time) proxy settings detected on the administrator's account during installation and which can be configured only if you are logged on to that account. If the proxy server requires a username and a password, you must specify them in the corresponding fields.
- Current user proxy settings (from default browser) proxy settings of the current user, extracted from the default browser. If the proxy server requires a username and a password, you must specify them in the corresponding fields.



Note

The supported web browsers are Internet Explorer, Mozilla Firefox and Opera. If you use another browser by default, BitDefender will not be able to obtain the proxy settings of the current user.

Your own set of proxy settings - proxy settings that you can configure if you are logged in as an administrator.



The following settings must be specified:

- Address type in the IP of the proxy server.
- Port type in the port BitDefender uses to connect to the proxy server.
- Username type in a user name recognized by the proxy.
- · Password type in the valid password of the previously specified user.

When trying to connect to the Internet, each set of proxy settings is tried at a time, until BitDefender manages to connect.

First, the set containing your own proxy settings will be used to connect to the Internet. If it does not work, the proxy settings detected at installation time will be tried next. Finally, if those do not work either, the proxy settings of the current user will be taken from the default browser and used to connect to the Internet.

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

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



23. Registration

To find complete information on your BitDefender product and the registration status, go to **Registration** in the Advanced View.

BitDefender Antiv	irus 2009 - Trial	SWITCH TO BASIC VIEW
STATUS: There is 1 per	ding issue	FIX ALL ISSUES
	Registration	
General		
Antivirus	Product Informations	
Privacy Control	BitDefender Antivirus 2009 Version: 12.0.8	
Vulnerability		
Encryption	Dedistration Information	
Game/Laptop Mode	Registration Information Expires in 30 days License key: 7046E277EF7785580DF8	
Network		
Update		
	Create an account Register now	
C This is data about your and register your produ	BitDefender version, about the registration and v ict if the case.	slidity of the license key. You can also create your BitDefender account
(Spitdefender)		Buy - My Account - Register - Help - Support - History
Registration		

This section displays:

- Product Information: the BitDefender product and version.
- Registration Information: the e-mail address used to log your BitDefender account (if configured), the current license key and how many days are left until the license expires.

23.1. Registering BitDefender Antivirus 2009

Click Register now to open the product registration window.



Bit Defender Antivirus 2009	_ x
Registration Wizard	
Step 1	
Welcome to the BitDefender Registration Wizard!	This is where you can find your
This wizard will help you register BitDefender and create or update your BitDefender Account	license key: 1) CD-Rom label
Your current BitDefender license status is: Trial	Enda de lovegisteren:
Your current BitDefender license key is: 704BE277EF7785580DF8	
This license key will expire in: 30 days	
	2) Product registration card
	Santa de loregistrares
 If you want to keep the current key, please select the rist option. If you want to add a new key, please select the second option and fill the key in the box below. Continue using the current key 	
I want to register the product with a new key	3) Online purchase e-mail
Enter a new license key:	
Buy a license key	Tania de Derganteres 2012/22/22/22/22/22/22/22/22/22/22/22/22/2
If you want to buy a license key, please visit our online store at:	1985. BYS
Renew Your BitDefender license Key	international and a second sec
The BRDefender Registration Wizard will help you register BRDefender and create or update y	our BitDefender Account.
Sitdefender	Finish Cancel
Registration	

You can see the BitDefender registration status, the current license key and how many days are left until the license expires.

To register BitDefender Antivirus 2009:

- 1. Select I want to register the product with a new key.
- 2. Type the license key in the edit field.



Note

- You can find your license key:
- on the CD label.
- on the product registration card.
- in the online purchase e-mail.

If you do not have a BitDefender license key, click the provided link to go to the BitDefender online store and buy one.

Click Finish.



23.2. Creating a BitDefender Account

As part of the registration process, you MUST create a BitDefender account. The BitDefender account gives you access to BitDefender updates, free technical support and special offers and promotions. If you loose your BitDefender license key, you can log in to your account at http://myaccount.bitdefender.com to retrieve it.



Important

You must create an account within 15 days after installing BitDefender (if you register it, the deadline is extended to 30 days). Otherwise, BitDefender will no longer update.

If you have not yet created a BitDefender account, click **Create an account** to open the account registration window.

Bit Defender Antivirus 2009	_ X	
Create Account		
Step 1		
My Account registration Information about an existing BitDefender account was f special offers and promotions. If you lose your BitDefend choose to sign in to an existing BitDefender Account or to	ound on this computer. The BitDefender Account gives you access to technical support and der license key you can retrieve it by logging in to http://myaccount.bitdefender.com. You can o create a new one.	
Sign in to an existing BitDefender Account	Create a new BitDefender Account	
E-mail address:	E-mail Address:	
Password:	Password:	
Forgot your password?	Re-Type password:	
	First Name:	
	Last Name:	
	Country:	
○ Skip registration		
	Send me all messages from BitDefender	
	Send me only the most important messages	
	O Don't send me any messages	
This is where you can create a new BitDefender acc to create an account later on	ount or login to your already existing one. If you choose to skip this step you will be reminded	
Sbitdefender	Finish Cancel	
ccount Creation		

If you do not want to create a BitDefender account at the moment, select **Skip** registration and click **Finish**. Otherwise, proceed according to your current situation:

• "I do not have a BitDefender account" (p. 198)



"I already have a BitDefender account" (p. 198)

I do not have a BitDefender account

To create a BitDefender account, select **Create a new BitDefender account** and provide the required information. The data you provide here will remain confidential.

- **E-mail address** type in your e-mail address.
- Password type in a password for your BitDefender account. The password must be at least six characters long.
- Re-type password type in again the previously specified password.
- First name type in your first name.
- **Last name** type in your last name.
- **Country** select the country you reside in.



Note

Use the provided e-mail address and password to log in to your account at http://myaccount.bitdefender.com.

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.

Optionally, BitDefender can inform you about special offers and promotions using the e-mail address of your account. Select one of the available options:

- Send me all messages from BitDefender
- Send me only the most important messages
- Don't send me any messages

Click Finish.

I already have a BitDefender account

BitDefender will automatically detect if you have previously registered a BitDefender account on your computer. In this case, provide the password of your account.

If you already have an active account, but BitDefender does not detect it, select **Sign in to an existing BitDefender Account** and provide the e-mail address and the password of your account.



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

Optionally, BitDefender can inform you about special offers and promotions using the e-mail address of your account. Select one of the available options:

- Send me all messages from BitDefender
- Send me only the most important messages
- Don't send me any messages

Click Finish.



Getting Help



24. Support

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.

24.1. 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.


24.2. Asking for Help

24.2.1. Go to Web Self Service

Got a question? Our security experts are available to help you 24/7 via phone, email or chat at no additional cost.

Please, follow the links below:

English

http://www.bitdefender.com/site/KnowledgeBase/

German

http://www.bitdefender.com/de/KnowledgeBase/

French

http://www.bitdefender.com/fr/KnowledgeBase/

Romanian

http://www.bitdefender.com/ro/KnowledgeBase/

Spanish

http://www.bitdefender.com/es/KnowledgeBase/

24.2.2. Open a support ticket

If you want to open a support ticket and receive help via email, just follow one of these links:

English: http://www.bitdefender.com/site/Main/contact/1/ German: http://www.bitdefender.de/site/Main/contact/1/ French: http://www.bitdefender.fr/site/Main/contact/1/ Romanian: http://www.bitdefender.ro/site/Main/contact/1/ Spanish: http://www.bitdefender.es/site/Main/contact/1/



24.3. Contact Information

Efficient communication is the key to a successful business. During the past 10 years BITDEFENDER 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.

24.3.1. 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/pub Local distributors: http://www.bitdefender.com/partner_list BitDefender Knowledge Base: http://kb.bitdefender.com

24.3.2. 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.

U.S.A

BitDefender, LLC

6301 NW 5th Way, Suite 3500 Fort Lauderdale, Florida 33309 Phone: 1-954-776-6262 Web: http://www.bitdefender.com

Technical Support (Registered Users Only):

- E-mail: support@bitdefender.com
- Phone (Toll-Free):



- United States: 1-888-868-1873
- Canada: 1-866-947-1873

Customer Service (Registered Users Only):

- E-mail: customerservice@bitdefender.com
- Phone (Toll-Free):
 - United States: 1-888-868-1873
 - · Canada: 1-866-947-1873

Germany

BitDefender GmbH

Airport Office Center Robert - Bosch - Str. 2 59439 Holzwickede Germany Tel: +49 (0)231 99 33 98 0 Email: info@bitdefender.com Sales: sales@bitdefender.com Web: http://www.bitdefender.com Technical Support: support@bitdefender.com

UK and Ireland

Business Centre 10 Queen Street Newcastle, Staffordshire ST5 1ED Tel: +44 (0) 8451-305096 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

Romania

BITDEFENDER

West Gate Park, Building H2, 24 Preciziei Street Bucharest Technical support: support@bitdefender.com Sales: sales@bitdefender.com Phone: +40 21 3001255 Phone: +40 21 3001254 Product web site: http://www.bitdefender.com



BitDefender Rescue CD



25. Overview

BitDefender Antivirus 2009 comes with a bootable CD (BitDefender Rescue CD) 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.

BitDefender Rescue CD is a BitDefender re-mastered Knoppix distribution, which integrates the latest BitDefender for Linux security solution into the GNU/Linux Knoppix Live CD, offering a desktop antivirus which can scan and disinfect existing hard drives (including Windows NTFS partitions). At the same time, BitDefender Rescue CD can be used to restore your valuable data when you cannot boot Windows.



Note

BitDefender Rescue CD can be downloaded from this location: http://download.bitdefender.com/rescue_cd/

25.1. System Requirements

Before booting BitDefender Rescue CD, 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

Minimum 512 MB of RAM Memory (1 GB recommended)

CD-ROM

BitDefender Rescue CD runs from a CD-ROM, therefore a CD-ROM and a BIOS capable to boot from it is required.

Internet connection

Although BitDefender Rescue CD 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

Standard SVGA-compatible graphics card.

25.2. Included Software

BitDefender Rescue CD includes the following software packages.

Xedit

This is a text file editor.

Vim

This is a powerful text file editor, containing syntax highlighting, a GUI, and much more. For more information, please refer to the Vim homepage.

Xcalc

This is a calculator.

RoxFiler

RoxFiler is a fast and powerful graphical file manager.

For more information, please refer to the RoxFiler homepage.

MidnightCommander

GNU Midnight Commander (mc) is a text-mode file manager.

For more information, please refer to the MC homepage.

Pstree

Pstree displays running processes.

Тор

Top displays Linux tasks.

Xkill

Xkill kills a client by its X resources.

Partition Image

Partition Image helps you save partitions in the EXT2, Reiserfs, NTFS, HPFS, FAT16, and FAT32 file system formats to an image file. This program can be useful for backup purposes.

For more information, please refer to the Partimage homepage.

GtkRecover

GtkRecover is a GTK version of the console program recover. It helps you recover a file.

For more information, please refer to the GtkRecover homepage.



ChkRootKit

ChkRootKit is a tool that helps you scan your computer for rootkits.

For more information, please refer to the ChkRootKit homepage.

Nessus Network Scanner

Nessus is a remote security scanner for Linux, Solaris, FreeBSD, and Mac OS X.

For more information, please refer to the Nessus homepage.

lptraf

Iptraf is an IP Network Monitoring Software.

For more information, please refer to the lptraf homepage.

lftop

Iftop displays bandwidth usage on an interface.

For more information, please refer to the Iftop homepage.

MTR

MTR is a network diagnostic tool.

For more information, please refer to the MTR homepage.

PPPStatus

PPPStatus displays statistics about the incoming and outgoing TCP/IP traffic.

For more information, please refer to the PPPStatus homepage.

Wavemon

Wavemon is a monitoring application for wireless network devices.

For more information, please refer to the Wavemon homepage.

USBView

USBView displays information about devices connected to the USB bus.

For more information, please refer to the USBView homepage.

Pppconfig

Pppconfig helps automatically setting up a dial up ppp connection.

DSL/PPPoe

DSL/PPPoe configures a PPPoE (ADSL) connection.

I810rotate

1810rotate toggles the video output on i810 hardware using i810switch(1).

For more information, please refer to the **I810rotate homepage**.



Mutt

Mutt is a powerful text-based MIME mail client.

For more information, please refer to the Mutt homepage.

Mozilla Firefox

Mozilla Firefox is a well-known web browser.

For more information, please refer to the Mozilla Firefox homepage.

Elinks

Elinks is a text mode web browser.

For more information please refer to the Elinks homepage.



26. BitDefender Rescue CD Howto

This chapter contains information on how to start and stop the BitDefender Rescue CD, scan your computer for malware as well as save data from your compromised Windows PC to a removable device. However, by using the software applications that come with the CD, you can do many tasks the description of which goes far beyond the scope of this user's guide.

26.1. Start BitDefender Rescue CD

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 BitDefender Rescue CD.



Note

Select the language you want to use for the Rescue CD from the available list.





At boot time, the update of the virus signatures is made automatically. This may take a while.

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



26.2. Stop BitDefender Rescue CD

You can safely shut down your computer by selecting **Exit** from the BitDefender Rescue CD contextual menu (right-click to open it) or by issuing the **halt** command in a terminal.



Choose "EXIT"

When BitDefender Rescue CD 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.



Wait for this message when shutting down

26.3. How do I perform an antivirus scan?

A wizard will appear when the boot process has finished and allow you to full scan your computer. All you have to do is click the **Start** button.



Note

If your screen resolution isn't high enough, you will be asked to start scanning in text-mode.

Follow the three-step guided procedure to complete the scanning process.

1. You can see the scan status and statistics (scanning speed, elapsed time, number of scanned / infected / suspicious / hidden objects and other).



Note

The scanning process may take a while, depending on the complexity of the scan.

2. You can see the number of issues affecting your system.

The issues are displayed in groups. Click the "+" box to open a group or the "-" box to close a group.

You can choose an overall action to be taken for each group of issues or you can select separate actions for each issue.



3. You can see the results summary.

If you want to scan certain directory only, do as follow:

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.

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

26.4. How do I 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. Double-click the Network Connections shortcut on the Desktop. The following window will appear.

Network Connections	- 🗆 ×
Current state: Online (ethO) Please select:	
modemlink (re)configure /dev/modem device	
netcardconfig LAN or wireless access	
gprsconnect Dial via cellphone/GPRS	
pppoeconf Dial via DSL-adapter	
🗸 OK 🗙 Quit	
Natwork Connections	

- Network Connections
- 2. Select the type of connection you are using and click OK.

Connection	Description
modemlink	Select this type of connection when you are using a modem and a telephone line to access the Internet.

Connection	Description
netcardconfig	Select this type of connection when you are using a local area network (LAN) to access the Internet. It is also suitable for wireless connections.
gprsconnect	Select this type of connection when you are accessing the Internet over a mobile phone network by using GPRS (General Packet Radio Service) protocol. Of course you can use also a GPRS modem instead of a mobile phone.
pppoeconf	Select this type of connection when you are using a DSL (Digital Subscriber Line) modem to access the Internet.

3. Follow the on-screen instructions. If you're not sure what to write, contact your system or network administrator for details.



Important

Please be aware that you only activate the modem by selecting the above-mentioned options. To configure the network connection follow these steps.

- 1. Right -click the Desktop. The BitDefender Rescue CD contextual menu will appear.
- 2. Select Terminal (as root).
- 3. Type the following commands:

pppconfig

4. Follow the on-screen instructions. If you're not sure what to write, contact your system or network administrator for details.

26.5. How do I update BitDefender?

At boot time, the update of the virus signatures is made automatically. But, if you skipped this step here's how to update BitDefender.

1. Double-click the Update Signatures shortcut on the Desktop. The following window will appear.



Update Signatures

- 2. Do one of the following:
 - Select Cumulative to install signatures already saved on your hard disk by browsing your computer and loading the cumulative.zip file.
 - Select Update to immediately connect to the internet and download the latest virus signatures.
- 3. Click **OK**.

26.5.1. How do I update BitDefender over a proxy?

If there is a proxy server between your computer and the Internet, some configurations were to be done in order to update the virus signatures.

To update BitDefender over a proxy just follow these steps:

- 1. Right -click the Desktop. The BitDefender Rescue CD contextual menu will appear.
- 2. Select Terminal (as root).
- 3. Type the command: cd /ramdisk/BitDefender-scanner/etc.
- 4. Type the command: **mcedit bdscan.conf** to edit this file by using GNU Midnight Commander (mc).
- 5. Uncomment the following line: #HttpProxy = (just delete the # sign) and specify the domain, username, password and server port of the proxy server. For example, the respective line must look like this:

HttpProxy = myuser:mypassword@proxy.company.com:8080

- 6. Press F2 to save the current file, confirm saving, and then press F10 to close it.
- 7. Type the command: bdscan update.

26.6. How do I save my data?

Let's assume that you cannot start your Windows PC due to some unknown issues. At the same time, you desperately need to access some important data from your computer. This is where BitDefender Rescue CD comes in handy.



To save your data from the computer to a removable device, such as an USB memory stick, just follow these steps:

1. Put the BitDefender Rescue CD in the CD drive, the memory stick into the USB drive and then restart the computer.



Note

If you plug the memory stick at a later moment, you have to mount the removable device by following these steps:

a. Double-click the Terminal Emulator shortcut on the Desktop.

b. Type the following command:

mount /media/sdb1

Please be aware that depending on your computer configuration it might be sdal instead of sdbl.

2. Wait until BitDefender Rescue CD finishes booting. The following window will appear.



3. Double-click the partition where the data you want to save is located (e.g. [sda3]).





Note

When working with BitDefender Rescue CD, you will deal with Linux-type partition names. So, [sda1] will probably correspond to the (C:) Windows-type partition, [sda3] to (F:), and [sdb1] to the memory stick.



Important

If the computer was not properly shut down, it is possible that certain partitions were not mounted automatically. To mount a partition, follow these steps.

- a. Double-click the Terminal Emulator shortcut on the Desktop.
- b. Type the following command:



- 4. Browse your folders and open the desired directory. For instance, MyData which contains Movies, Music and E-books sub-directories.
- 5. Right-click the desired directory and select Copy. The following window will appear.



6. Type /media/sdb1/ into the corresponding textbox and click Copy.

Please be aware that depending on your computer configuration it might be ${\tt sdal}$ instead of ${\tt sdbl}.$



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 it's own update module that allows you to manually check for updates, or let it automatically update the product.

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Virus definition

The binary pattern of a virus, used by the antivirus program to detect and eliminate the virus.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.