

*bit*defender



GAMESAFE

User's guide

BitDefender GameSafe

User's guide

Published 2008.03.19

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

License and Warranty	viii
Preface	xii
1. Conventions Used in This Book	xii
1.1. Typographical Conventions	xii
1.2. Admonitions	xiii
2. The Book Structure	xiii
3. Request for Comments	xiv
Installation	1
1. BitDefender GameSafe Installation	2
1.1. System Requirements	2
1.2. Installation Steps	3
1.3. Initial Setup Wizard	5
1.3.1. Step 1/6 - Register BitDefender GameSafe	6
1.3.2. Step 2/6 - Create a BitDefender Account	7
1.3.3. Step 3/6 - Learn about Real-Time Virus Reporting (RTVR)	9
1.3.4. Step 4/6 - Select the Tasks to Be Run	10
1.3.5. Step 5/6 - Wait for the Tasks to Complete	11
1.3.6. Step 6/6 - View Summary	12
1.4. Upgrade	12
1.5. Repairing or Removing BitDefender	12
Basic Administration	14
2. Getting Started	15
2.1. BitDefender Icon in the System Tray	16
2.2. Scan Activity Bar	17
2.3. BitDefender Manual Scan	17
2.4. Game Mode	18
2.4.1. Using Game Mode	18
2.4.2. Changing Game Mode Hotkey	19
3. Security Status	20
3.1. PC Security Status Button	22
3.2. Network Security Status Button	22
3.3. Identity Control Status Button	23
4. Quick Tasks	24
4.1. Security	24
4.1.1. Updating BitDefender	24
4.1.2. Scanning with BitDefender	26

5. History	31
6. Registration	33
6.1. Step 1/3 - Register BitDefender GameSafe	33
6.2. Step 2/3 - Create a BitDefender Account	34
6.3. Step 3/3 - Register BitDefender GameSafe	36
Advanced Security Administration	37
7. Settings Console	38
7.1. Configuring General Settings	39
7.1.1. General Settings	40
7.1.2. Virus Report Settings	41
7.1.3. Manage Settings	41
8. Antivirus	42
8.1. On-access Scanning	42
8.1.1. Configuring Protection Level	43
8.1.2. Customizing Protection Level	44
8.1.3. Disabling Real-time Protection	48
8.2. On-demand Scanning	48
8.2.1. Scan Tasks	49
8.2.2. Using Shortcut Menu	51
8.2.3. Creating Scan Tasks	52
8.2.4. Configuring Scan Tasks	52
8.2.5. Scanning Objects	63
8.2.6. Viewing Scan Logs	70
8.3. Objects Excluded from Scanning	71
8.3.1. Excluding Paths from Scanning	73
8.3.2. Excluding Extensions from Scanning	76
8.4. Quarantine Area	78
8.4.1. Managing Quarantined Files	79
8.4.2. Configuring Quarantine Settings	80
9. Firewall	82
9.1. Firewall Insights	82
9.1.1. What Are Firewall Profiles?	82
9.1.2. What Are Network Zones?	84
9.1.3. Firewall Operation	85
9.2. Firewall Status	86
9.2.1. Configuring Protection Level	88
9.3. Traffic Control	88
9.3.1. Adding Rules Automatically	89
9.3.2. Adding Rules Manually	90
9.3.3. Managing Rules	95
9.3.4. Modifying Profiles	95

9.3.5. Resetting Profiles	97
9.4. Advanced Settings	98
9.4.1. Configuring ICMP Filtering Settings	99
9.4.2. Configuring Advanced Firewall Settings	100
9.5. Connection Control	102
9.6. Network Zones	104
9.6.1. Adding Zones	106
10. Privacy Control	107
10.1. Privacy Control Status	107
10.1.1. Privacy Control	108
10.1.2. Antiphishing Protection	109
10.2. Advanced Settings - Identity Control	110
10.2.1. Creating Identity Rules	111
10.2.2. Defining Exceptions	114
10.2.3. Managing Rules	115
10.3. Advanced Settings - Registry Control	116
10.4. Advanced Settings - Cookie Control	118
10.4.1. Configuration Wizard	120
10.5. Advanced Settings - Script Control	122
10.5.1. Configuration Wizard	123
10.6. System Information	124
10.7. Antiphishing Toolbar	126
11. Update	128
11.1. Automatic Update	128
11.1.1. Requesting an Update	130
11.1.2. Disabling Automatic Update	130
11.2. Update Settings	131
11.2.1. Setting Update Locations	131
11.2.2. Configuring Automatic Update	132
11.2.3. Configuring Manual Update	133
11.2.4. Configuring Advanced Settings	133
11.2.5. Managing Proxies	134
BitDefender Rescue CD	136
12. Overview	137
12.1. System Requirements	137
12.2. Included Software	138
13. BitDefender Rescue CD Howto	141
13.1. Start BitDefender Rescue CD	141
13.2. Stop BitDefender Rescue CD	142
13.3. How do I perform an antivirus scan?	143
13.4. How do I update BitDefender over a proxy?	144

13.5. How do I save my data? 144

Getting Help 147

14. Support 148

14.1. BitDefender Knowledge Base 148

14.2. Asking for Help 149

14.2.1. Go to Web Self Service 149

14.3. Contact Information 149

14.3.1. Web Addresses 149

14.3.2. Branch Offices 149

Glossary 152

License and Warranty

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

These Terms cover BitDefender Solutions and Services for 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.

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 5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, or at Tel No: 40-21-2330780 or Fax:40-21-2330763, e-mail address: office@bitdefender.com.

Preface

This guide is intended to all users who have chosen **BitDefender GameSafe** 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 GameSafe**, 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 GameSafe**, 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.

<i>Appearance</i>	<i>Description</i>
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. xii)	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.
<code>sample code listing</code>	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 GameSafe**. Starting with the prerequisites for a successful 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 Security Administration. A detailed presentation of the security capabilities provided by BitDefender. The chapters explain in detail all options of the advanced settings console. 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).

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

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

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

3. Request for Comments

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

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



Important

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

Installation

1. BitDefender GameSafe Installation

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

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

1.1. System Requirements

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

- Operating platform: Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (or higher)

Windows 2000

- 800 MHz processor or higher
- Minimum 256 MB of RAM Memory (512 MB recommended)
- Minimum 60 MB available hard disk space

Windows XP

- 800 MHz processor or higher
- Minimum 256 MB of RAM Memory (1 GB recommended)
- Minimum 60 MB available hard disk space

Windows Vista

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

BitDefender GameSafe can be downloaded for evaluation from the BitDefender website: <http://www.bitdefender.com>.

1.2. Installation Steps

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

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.



Installation Steps

Follow these steps to install BitDefender GameSafe:

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

BitDefender GameSafe 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, select **I accept the terms in the License Agreement** and click **Next**. If you do not agree with these terms click **Cancel**. The installation process will be abandoned and you will exit setup.
4. By default, BitDefender GameSafe will be installed in `C:\Program Files\BitDefender\BitDefender 2008`. If you want to change the installation path, click **Browse** and select the folder in which you would like BitDefender GameSafe 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 GameSafe 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 Firewall** - to turn off Windows Firewall.



Important

We recommend you to turn off Windows Firewall since BitDefender GameSafe already includes an advanced firewall. Running two firewalls on the same computer may cause problems.

- **Turn off Windows Defender** - to turn off Windows Defender; this option appears only on Windows Vista.

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



Important

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

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

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.

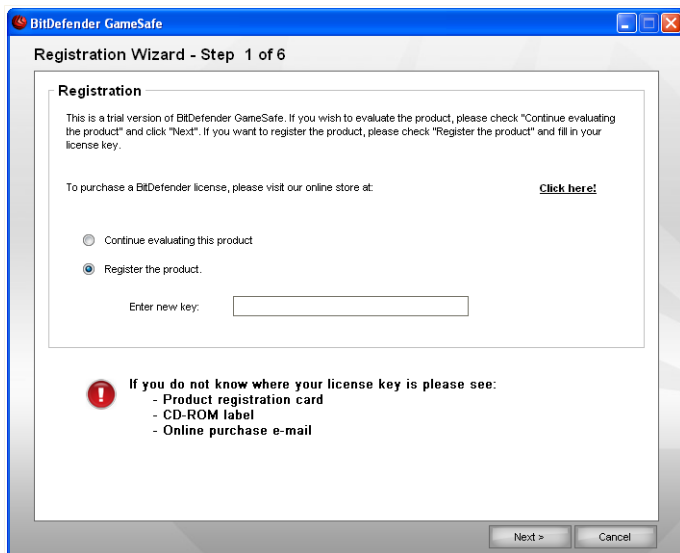
If you have accepted the default settings for the installation path, you can see in `Program Files` a new folder, named `BitDefender`, which contains the subfolder `BitDefender 2008`.

1.3. Initial Setup Wizard

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

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

1.3.1. Step 1/6 - Register BitDefender GameSafe



Registration

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

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

Click **Next**.

1.3.2. Step 2/6 - Create a BitDefender Account

Account Creation

I do not have a BitDefender account

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



Note

If you want to create an account later, select the corresponding option.

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** - type in your e-mail address.
- **Password** - type in a password for your BitDefender account.



Note

The password must be at least four 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.

Click **Next** to continue.

I already have a BitDefender account

BitDefender will automatically detect if you have previously registered a BitDefender account on your computer. In this case, all you have to do is to click **Next**.

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.



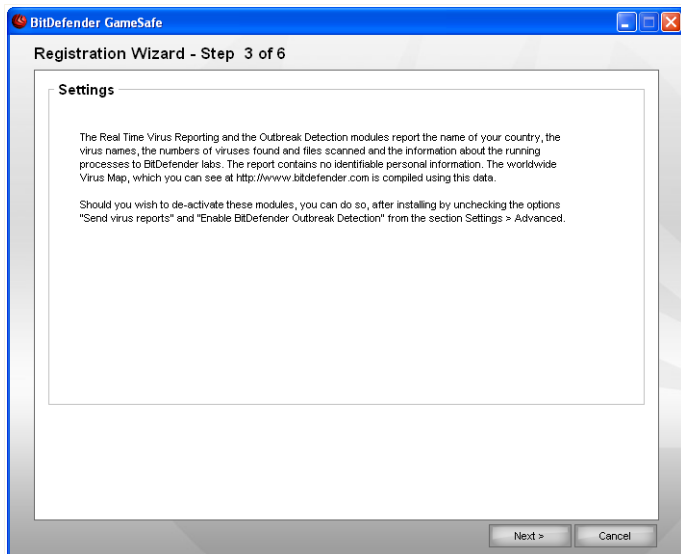
Note

If you provide an incorrect password, you will be prompted to re-type it when you click **Next**. Click **Ok** to enter the password again or **Cancel** to exit the wizard.

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

Click **Next** to continue.

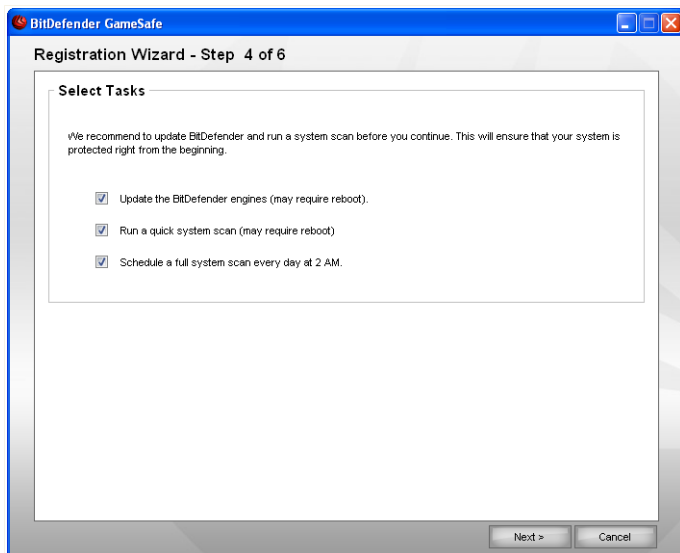
1.3.3. Step 3/6 - Learn about Real-Time Virus Reporting (RTVR)



RTVR Information

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

1.3.4. Step 4/6 - Select the Tasks to Be Run



Task Selection

Set BitDefender GameSafe 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.

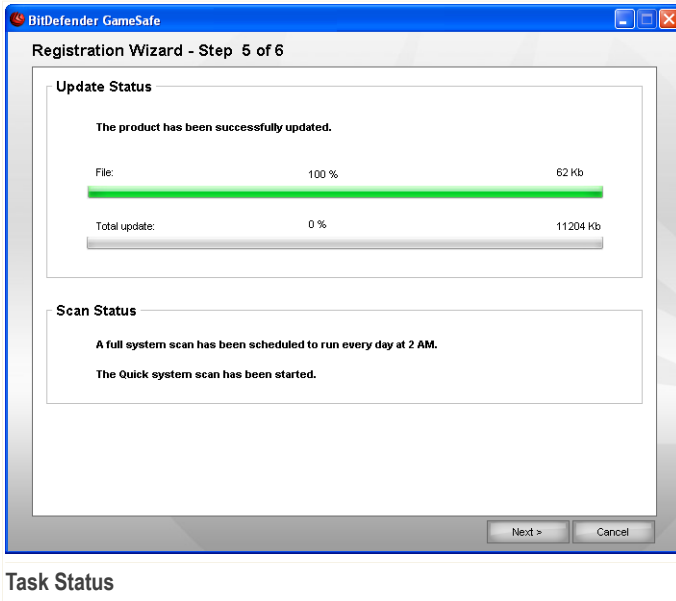


Important

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 or **Cancel** to exit the wizard.

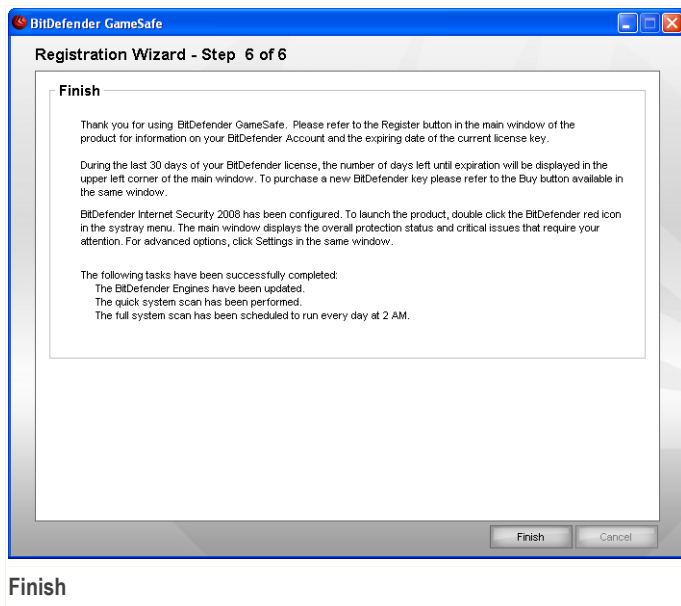
1.3.5. Step 5/6 - Wait for the Tasks to Complete



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

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

1.3.6. Step 6/6 - View Summary



This is the final step of the configuration wizard.

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

1.4. Upgrade

The upgrade procedure can be done in this way:

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

First, you must remove your previous version, then restart the computer and install the new one as described in the *“Installation Steps”* (p. 3) section.

1.5. Repairing or Removing BitDefender

If you want to repair or remove **BitDefender GameSafe**, follow the path from the Windows start menu: **Start** → **Programs** → **BitDefender 2008** → **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 GameSafe.

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

By removing BitDefender, you will no longer be protected against viruses, spyware and hackers. If you want Windows Firewall and Windows Defender (only on Windows Vista) to be enabled after uninstalling BitDefender, select the corresponding check boxes.

Click **Remove** to start the removal of BitDefender GameSafe 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 BitDefender folder from Program Files.


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

2. Getting Started

Once you have installed BitDefender your computer is protected. You can open the BitDefender Security Center to check the system security status, take preventive measures or fully configure the product at any time.

To access the BitDefender Security Center, use the Windows Start menu, by following the path **Start** → **Programs** → **BitDefender 2008** → **BitDefender GameSafe** or quicker, double click the  **BitDefender icon** in the system tray.



BitDefender Security Center

The BitDefender Security Center contains two areas:

- The **Status** area: contains information about and helps you fix the security vulnerabilities of your computer. You can easily see how many issues might affect your computer. By clicking the corresponding red **Fix All Issues** button your computer's vulnerabilities will be solved on the spot or you will be guided to easily fix them. At the same time, four status buttons corresponding to four security categories are available. Green status buttons indicate that there is no risk. Yellow

or Red buttons indicate medium or high security risks. To fix them, click the yellow/red button, and then the **Fix** buttons, one by one or the **Fix all now** button. Gray indicates a non-configured component.

- The **Quick Tasks** area: helps you keep your system safe and protect your data.

Furthermore, the BitDefender Security Center contains several useful shortcuts.

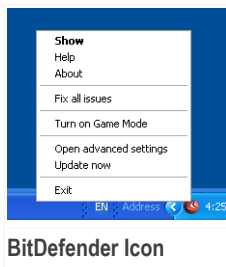
<i>Link</i>	<i>Description</i>
Buy	Opens a page where you can buy the product from.
My Account	Opens your BitDefender account page.
Register	Opens the registration wizard.
Help	Opens the help file.
Support	Opens the BitDefender support web page.
Settings	Opens the advanced settings console.
History	Opens a window with BitDefender history & events.

2.1. 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 Security Center will open. Also, by right-clicking the icon, a contextual menu will allow you to quickly manage the BitDefender product.

- **Show** - opens the BitDefender Security Center.
- **Help** - opens the help file.
- **About** - opens the BitDefender web page.
- **Fix all issues** - helps you remove security vulnerabilities.
- **Turn on / off Game Mode** - turns **Game Mode** on / off.
- **Open advanced settings** - gives access to advanced settings console.
- **Update now** - starts an immediate update. A new window will appear where you can see the update status.
- **Exit** - shuts down the application.



Whenever Game Mode is on, you can see the letter **G** over the  BitDefender icon.

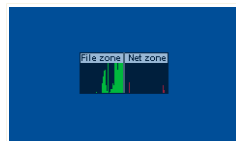
If there are critical issues affecting the security of your system, an exclamation mark is displayed over the  BitDefender icon. You can hover the mouse over the icon to see the number of issues affecting the system's security.

2.2. Scan Activity Bar

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

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

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



Activity Bar



Note

The Scan activity bar will notify you when real-time protection or the Firewall is disabled by displaying a red cross over the corresponding area (**File Zone** or **Net Zone**).

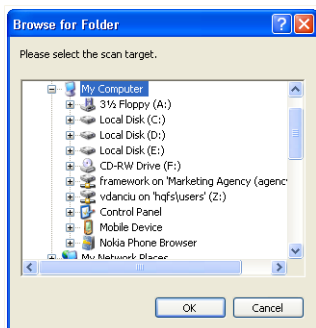
You can use the **Scan activity bar** to scan objects. Just drag the objects that you want to be scanned and drop them over it. For more information, please refer to *“Drag&Drop Scanning”* (p. 64).

When you no longer want to see the graphic visualization, just right-click it and select **Hide**. To completely hide this window, click **Advanced** in the settings console and clear the check box corresponding to **Enable the Scan Activity bar (on screen graph of product activity)**.

2.3. 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** → **Programs** → **BitDefender 2008** → **BitDefender Manual Scan**. The following window will appear:



BitDefender Manual Scan

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.

2.4. Game Mode

The new Game Mode temporarily modifies protection settings so as to minimize their impact on system performance. When you turn on the 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**.
- The BitDefender Firewall is set to **Game Mode**.

Whenever Game Mode is on, you can see the letter **G** over the  BitDefender icon.

2.4.1. 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 **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.

2.4.2. Changing Game Mode Hotkey

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

1. Click **Settings** in the BitDefender Security Center to open the settings console.



Note

You can also right-click the BitDefender icon in the system tray and select **Open advanced settings**.

2. Click **Advanced**.
3. Under the **Enable HotKey for Game Mode** 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**.



Note

Removing the checkmark next to **Enable HotKey for Game Mode** will disable the hotkey.

3. Security Status

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

There are three security status buttons:

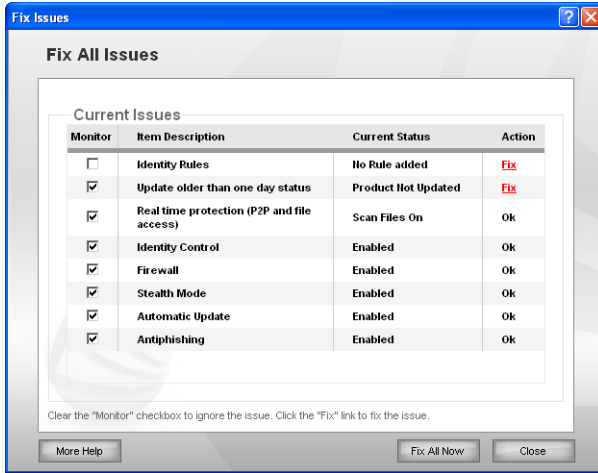
- **PC SECURITY**
- **NETWORK SECURITY**
- **IDENTITY CONTROL**

At the same time, on the left you can see the number of issues affecting the security of your system and a red **Fix All Issues** button.

The three status buttons can be displayed in green, yellow, red or grey, depending on the current level of protection.

- **Green** indicates a low security risk for your computer.
- **Yellow** indicates a medium security risk for your computer.
- **Red** indicates a high security risk for your computer.
- **Grey** indicates a non-configured component.

Fixing security problems requires no effort and it can be done by a single click on the **Fix All Issues** button. A new window will appear.



Security Issues

You can see a list of security issues and a short description of their status.

To fix only a particular issue click the corresponding **Fix** button. It will be solved either on the spot or after you follow the steps of a wizard. If you decide to fix them all, click the **Fix All Now** button and follow the corresponding wizard.

If you need additional help, click the **More Help** button, placed at the bottom of the window. A contextual help page is displayed providing you with detailed information about these issues and how to fix them.



Important

For every issue, there is a check box, enabled by default. If you do not want a specific issue to be taken into account when calculating the security risk, clear the corresponding check box. Please use this option with caution, as it is very easy to increase the security risk your computer is exposed to.

To fix the issues later, click **Close**.

3.1. PC Security Status Button

If the security status button is green, there is nothing to worry about. Otherwise, if the button is yellow, red or gray, there is a medium or high security risk your computer is exposed to.

The color of the status buttons can change not only when you configure the settings that might affect your computer's security, but when you forget to do important tasks. For example, if your last system scan is old, the security status button will be yellow. If it is very old, it will be red.

The table below will provide you with information about what elements are taken into account when calculating the security risk.

<i>Issue</i>	<i>Color</i>
The last system scan is old	Yellow
The last system scan is very old	Red
The real-time protection is disabled	Red
The antivirus protection level is set to permissive	Yellow
Automatic update is disabled	Red
The last update is one day old	Red

To fix the issues, follow these steps:

1. Click the security status button.
2. Click either the **Fix** buttons to fix them one by one or the **Fix All Now** button to fix them all at once.
3. If one issue is not fixed on the spot, follow the wizard to fix it.

3.2. Network Security Status Button

If the network security status button is green there is nothing to worry about. Otherwise, if the button is red, there is a high security risk your computer is exposed to.

The table below will provide you with information about what elements are taken into account when calculating the security risk.

<i>Issue</i>	<i>Color</i>
The firewall is disabled	Red
The stealth mode is disabled	Red
The wireless connection is not secured	Red

To fix the issues, follow these steps:

1. Click the network security status button.
2. Click either the **Fix** buttons to fix them one by one or the **Fix All Now** button to fix them all at once.
3. If one issue is not fixed on the spot, follow the wizard to fix it.

3.3. Identity Control Status Button

If the identity control status button is green, there is nothing to worry about. Otherwise, if the button is red or gray, there is a high security risk your computer is exposed to.

The table below will provide you with information about what elements are taken into account when calculating the security risk.

<i>Issue</i>	<i>Color</i>
The privacy protection is set and ON	Green
The privacy protection is set and OFF	Red
The privacy protection is not set	Gray

To fix the issues, follow these steps:

1. Click the privacy status button.
2. Click either the **Fix** buttons to fix them one by one or the **Fix All Now** button to fix them all at once.
3. If one issue is not fixed on the spot, follow the wizard to fix it.

4. Quick Tasks

Under the three status buttons there is the **Quick Tasks** area.

4.1. Security

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

To enter the Security module, click the **Security** tab.

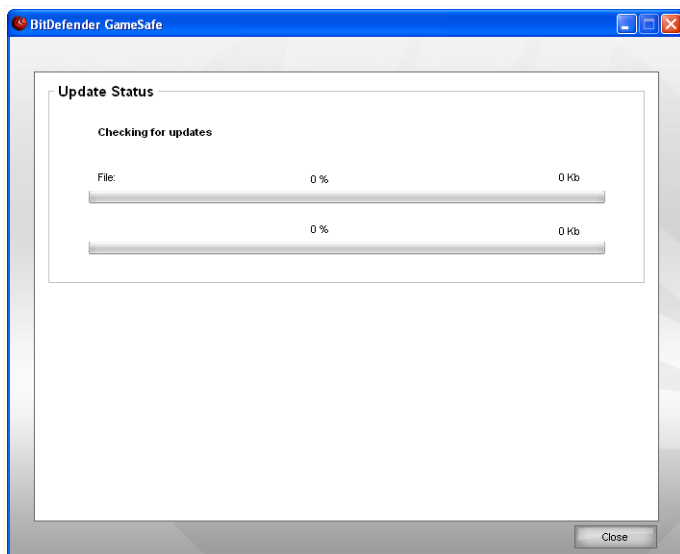
The following buttons are available:

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

4.1.1. 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:



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 **Close**. 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. If you do not want to be prompted anymore when an update requires a reboot, check **Wait for reboot, instead of prompting**. In this way, the next time when an update requires a reboot, the product will keep working with the old files until you reboot the system voluntarily.

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.

4.1.2. 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
Scan My Documents	Use this task to scan important current user folders: <i>My Documents</i> , <i>Desktop</i> and <i>StartUp</i> . This will ensure the safety of your documents, a safe workspace and clean applications running at startup.
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.



Note

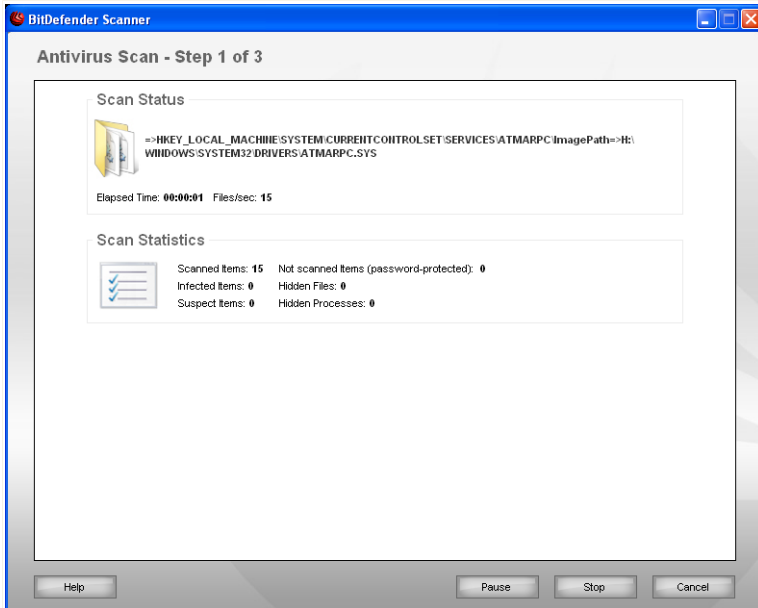
Since the **Deep System Scan** and **Full System Scan** tasks analyze the entire system, the scanning may take a while. Therefore, we recommend you to run these tasks on low priority or, better, when your system is idle.

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.

Step 1/3 - Scanning

BitDefender will start scanning the selected objects.



Scanning

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.

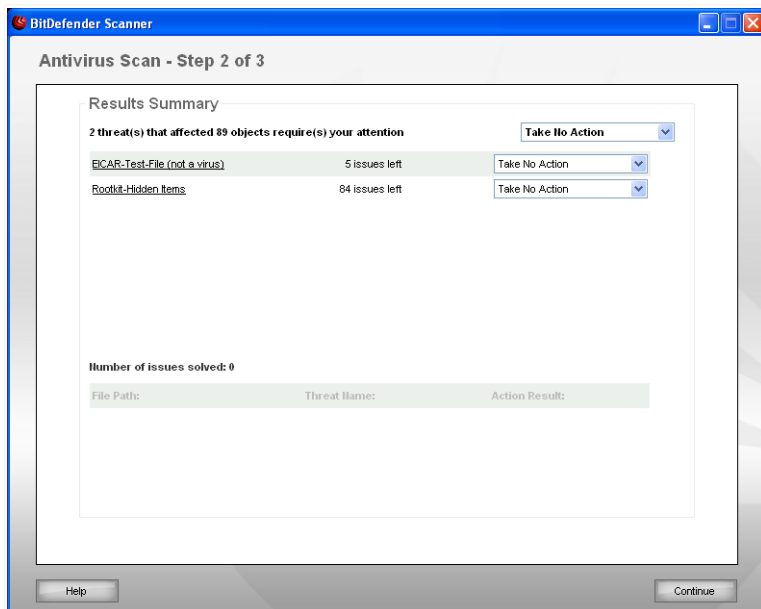
To temporarily stop the scanning process, just click **Pause**. You will have to click **Resume** to resume scanning.

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.



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 each group of issues or you can select separate actions for each issue.

The following options can appear on the menu:

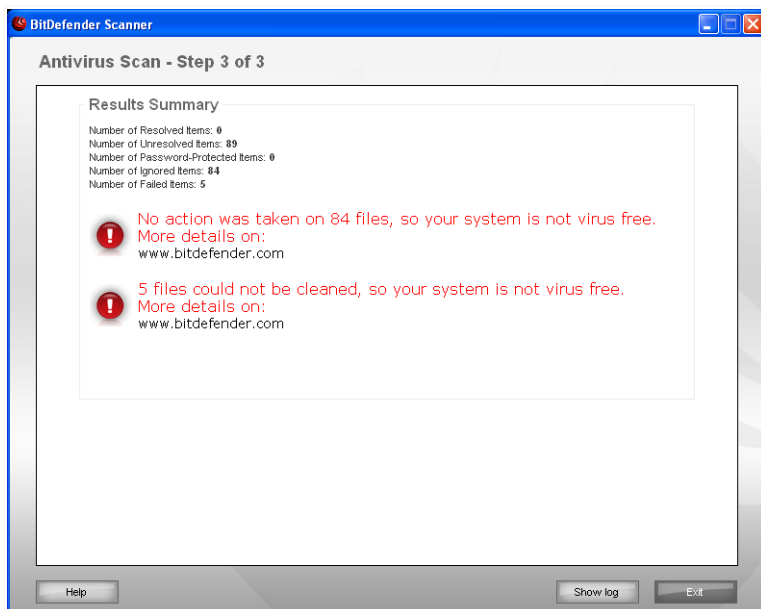
Action	Description
Take No Action	No action will be taken on the detected files.

Action	Description
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.



Summary

You can see the results summary. The report file is automatically saved in the **Logs** section from the **Properties** window of the respective task.



Important

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

Click **Exit** to close the results 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 Password-protected Items

The password-protected category includes two types of items: archives and installers. They do not present a real threat to the security of the system unless they contain infected files and only if executed.

To make sure that these items are clean:

- If the password-protected item is an archive you protected with a password, extract the files it contains and scan them separately. The easiest way to scan them is to right-click them and select **BitDefender Antivirus 2008** from the menu.
- If the password-protected item is an installer, make sure that **real-time protection** is enabled before you execute the installer. If the installer is infected, BitDefender will detect and isolate the infection.

If you do not want these objects to be detected again by BitDefender you must add them as exceptions to the scanning process. To add scan exceptions, click **Settings** to open the settings console and then go to **Antivirus > Exceptions** . For more information, please refer to [Objects Excluded from Scanning](#).

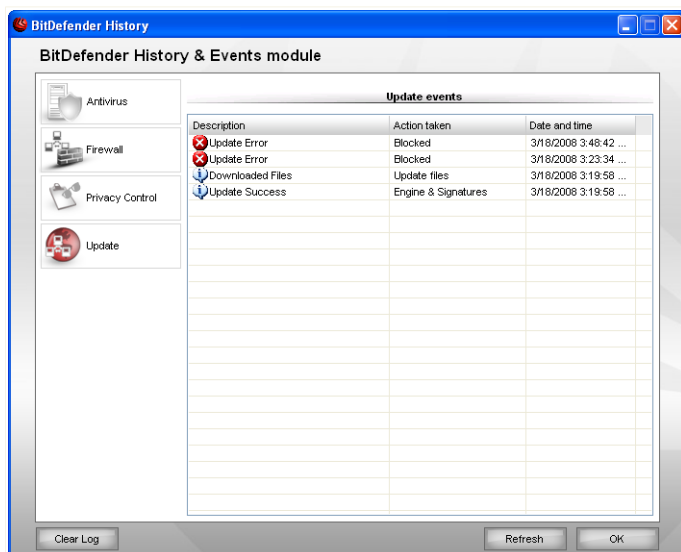
BitDefender Detected Suspect Files

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.

5. 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.



Events

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

- Antivirus
- Firewall
- Privacy Control
- Update

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,

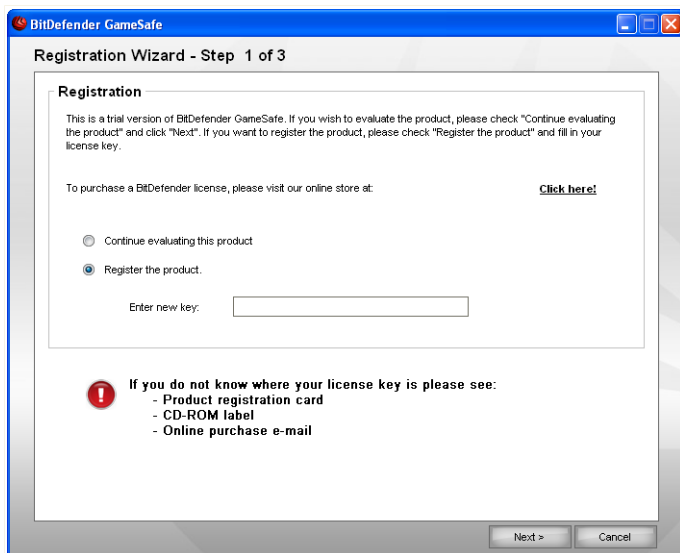
and the date and time when it occurred. If you want to find out more information about a particular event in the list, double click that event.

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

6. Registration

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

6.1. Step 1/3 - Register BitDefender GameSafe



Registration

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

To register BitDefender GameSafe, select **Register the product** and type the license key in the **Enter new key** field.

If the trial period has not expired and you want to continue evaluating the product, select **Continue evaluating the product**.

Click **Next** to continue.

6.2. Step 2/3 - Create a BitDefender Account

Register the Product

Information about an existing BitDefender account was found on this PC. The BitDefender account gives you access to technical support and special offers and promotions. Click "Next" to proceed with the registration process using this account.

Sign in to an existing BitDefender Account

E-mail:

Password: [Forgot your password?](#)

Create a new BitDefender Account

E-mail:

Password:

Retype password:

First name:

Last name:

Country:

Next > Cancel

Account Creation

I do not have a BitDefender account

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



Note

If you want to create an account later, select the corresponding option.

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** - type in your e-mail address.
- **Password** - type in a password for your BitDefender account.



Note

The password must be at least four 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.

Click **Next** to continue.

I already have a BitDefender account

BitDefender will automatically detect if you have previously registered a BitDefender account on your computer. In this case, all you have to do is to click **Next**.

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.



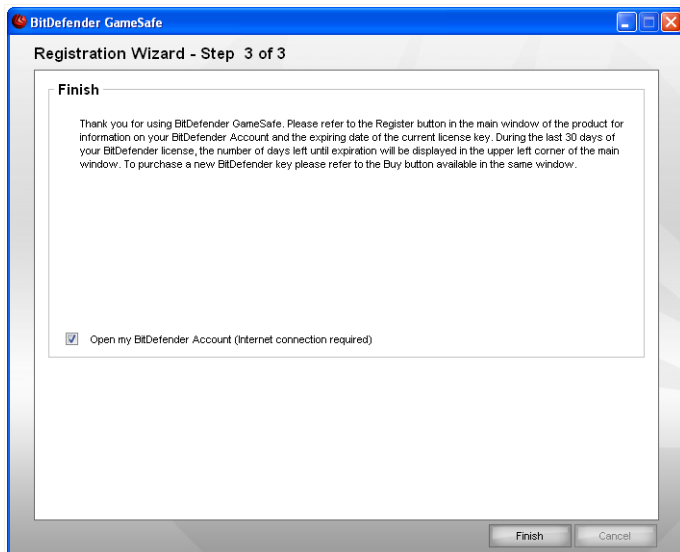
Note

If you provide an incorrect password, you will be prompted to re-type it when you click **Next**. Click **Ok** to enter the password again or **Cancel** to exit the wizard.

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

Click **Next** to continue.

6.3. Step 3/3 - Register BitDefender GameSafe



Summary

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

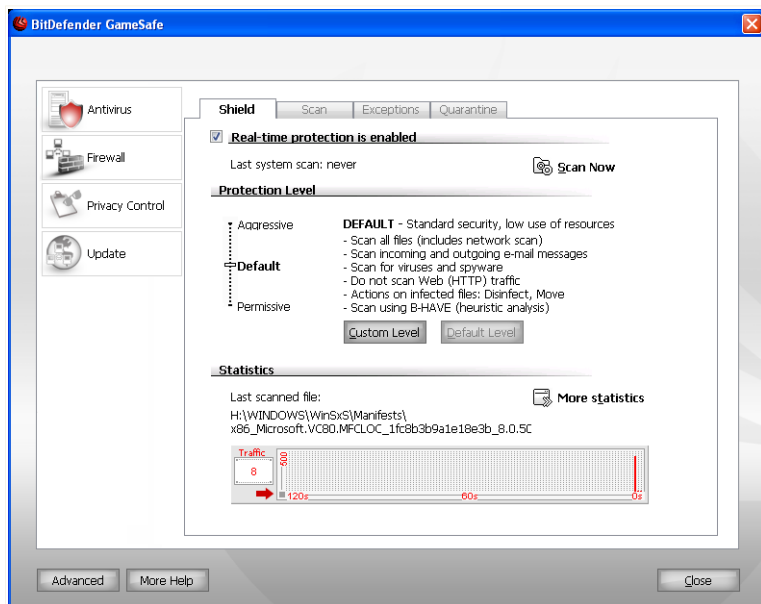
Click **Finish** to close the window.

Advanced Security Administration

7. Settings Console

BitDefender GameSafe comes with a centralized settings console, which allows advanced configuration and administration of BitDefender.

To access the settings console, click the **Settings** link, located at the bottom of the Security Center.



Settings Console

The settings console is organized into modules: **Antivirus**, **Privacy Control**, **Firewall** and **Update**. This allows you to easily manage BitDefender based on the type of security issue addressed.

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

- **Antivirus** - in this section you can configure the **Antivirus** module.
- **Firewall** - in this section you can configure the **Firewall** module.
- **Privacy Control** - in this section you can configure the **Privacy Control** module.

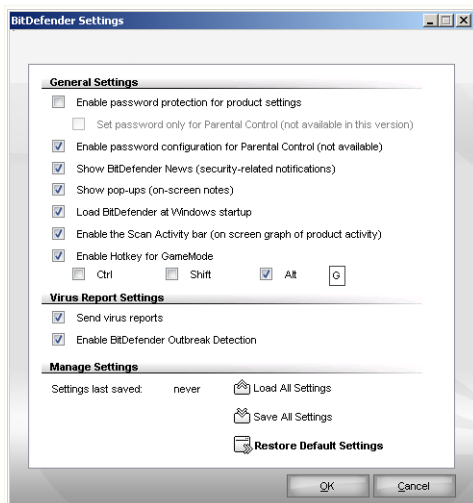
- **Update** - in this section you can configure the **Update** module.

At the bottom of the settings console, there is a **More Help** button that opens a contextual help page. Click this button to find out more information about the section you are into, whenever you need additional help.

If you need additional help, click the **More Help** button, placed at the bottom of the window. A contextual help page is displayed providing you with detailed information about the section you are into.

7.1. Configuring General Settings

To configure general settings for BitDefender GameSafe and to manage its settings, click **Advanced**. A new window will appear.



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.

7.1.1. General Settings

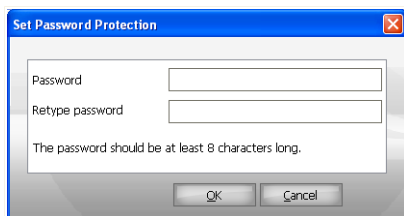
- **Enable password protection for product settings** - enables setting a password in order to protect the BitDefender configuration.



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:



Enter password

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.



Important

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

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



Note

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

- **Enable Hotkey for Game Mode** - allows using a combination of keyboard keys (hotkey) to enable / disable Game Mode. The default hotkey is **Alt+G**.

To modify the hotkey, do the following:

1. Check the modifier keys you want to use from the following: Control key (Ctrl), Shift key (Shift) or Alternate key (Alt).
2. In the edit field, type the letter corresponding to the regular key you want to use.

7.1.2. Virus Report Settings



- **Send virus reports** - sends to the BitDefender Labs reports regarding viruses identified in your computer. It helps us keep track of virus-outbreaks.

The reports will contain no confidential data, such as your name, IP address or others, and will not be used for commercial purposes. The information supplied will contain only the virus name and will be used solely to create statistic reports.

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

The reports will contain no confidential data, such as your name, IP address or others, and will not be used for commercial purposes. The information supplied will contain only the potential virus and will be used solely to detect new viruses.

7.1.3. Manage Settings

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



Important

Only users with administrative rights can save and load settings.

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

8. Antivirus

BitDefender protects your computer from all kinds of malware (viruses, Trojans, spyware, rootkits and so on).

Besides the classical scanning based on malware signatures, BitDefender will also perform a heuristic analysis on the scanned files. The aim of heuristic scanning is to identify new viruses, based on certain patterns and algorithms, before a virus definition is found. False alarm messages can appear. When such a file is detected it is classified as suspicious. In these cases, we recommend you to send the file to the BitDefender lab to be analyzed.

The protection BitDefender offers is divided into two categories:

- **On-access scanning** - prevents new malware threats from entering your system. This is also called real-time protection - files are scanned as you use them - on-access. BitDefender will, for example, scan a word document for known threats when you open it, and an e-mail message when you receive one.
- **On-demand scanning** - allows detecting and removing malware already residing in your system. This is the classic scan initiated by the user - you choose what drive, folder or file BitDefender should scan, and BitDefender scans it - on-demand. The scan tasks allow you to create customized scanning routines and they can be scheduled to run on a regular basis.

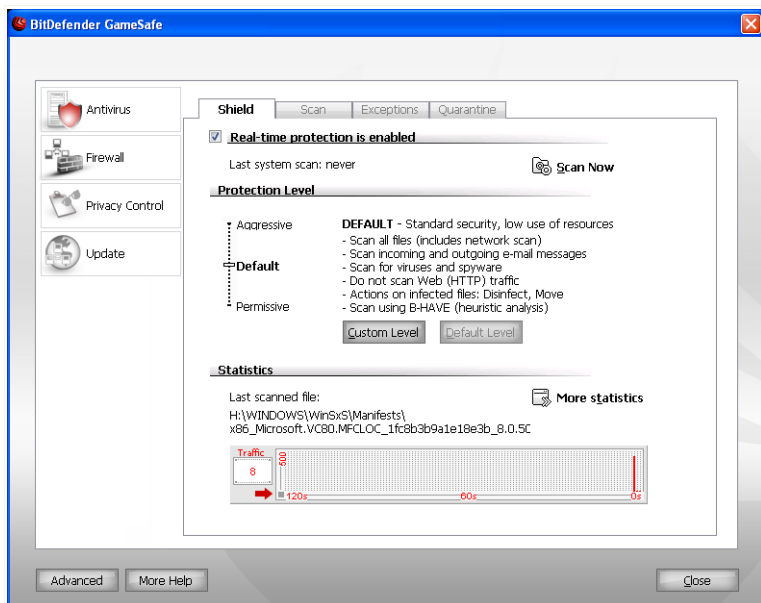
The **Antivirus** section of this user guide contains the following topics:

- [On-access Scanning](#)
- [On-demand Scanning](#)
- [Objects Excluded from Scanning](#)
- [Quarantine](#)

8.1. On-access Scanning

On-access scanning, also known as real-time protection, keeps your computer safe from all kinds 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).

To configure and monitor real-time protection, click **Antivirus>Shield** in the settings console. The following window will appear:



Real-time Protection



Important

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

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

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

8.1.1. 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:

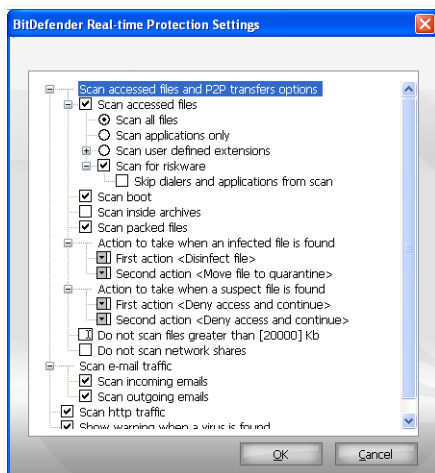
Protection level	Description
Permissive	Covers basic security needs. The resource consumption level is very low. Programs and incoming mail messages are only scanned for viruses. Besides the classical signature-based scan, the heuristic analysis is also used. The actions taken on infected files are the 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**.

8.1.2. 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;

Option	Description
	<p>.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.</p> <p>Scan user defined extensions Only the files with the extensions specified by the user will be scanned. These extensions must be separated by ",".</p> <p>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.</p> <p>Select Skip dialers and applications from scan if you want to exclude these kind of files from scanning.</p>
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	<p>Select from the drop-down menu the first action to take on infected and suspicious files.</p> <p>Deny access and continue In case an infected file is detected, the access to this will be denied.</p> <p>Clean file Disinfects infected files.</p> <p>Delete file Deletes infected files immediately, without any warning.</p> <p>Move file to quarantine Moves infected files into the quarantine.</p>

<i>Option</i>	<i>Description</i>
S e c o n d action	Select from the drop-down menu the second action to take on infected files, in case the first action fails.
Deny access and continue	In case an infected file is detected, the access to this will be denied.
Delete file	Deletes infected files immediately, without any warning.
Move file to quarantine	Moves infected files into the quarantine.
Do not scan files greater than [x] Kb	Type in the maximum size of the files to be scanned. If the size is 0 Kb, all files will be scanned, regardless their size.
Do not scan network shares	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:

<i>Option</i>	<i>Description</i>
Scan incoming mails	Scans all incoming e-mail messages.
Scan outgoing mails	Scans all outgoing e-mail messages.

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

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

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

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

8.1.3. Disabling Real-time Protection

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



Disable Real-time Protection

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

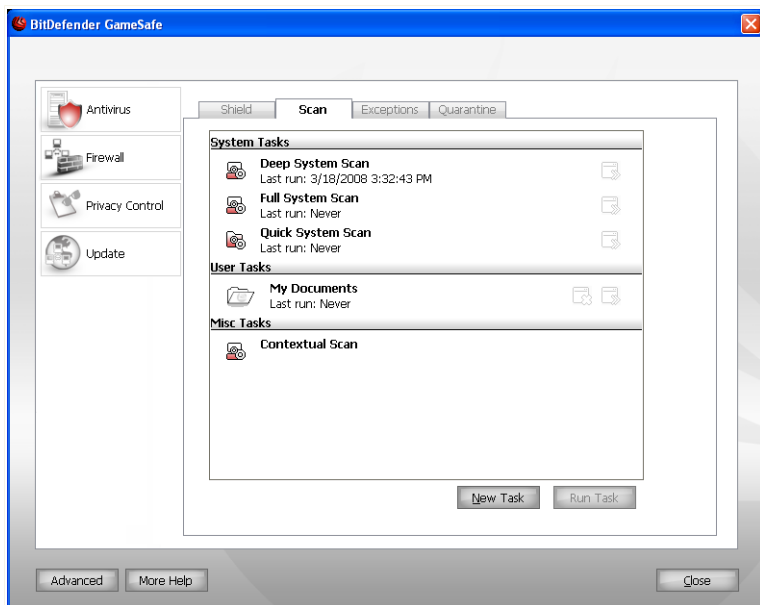
This is a critical security issue. We recommend you to disable real-time protection for as little time as possible. If real-time protection is disabled, you will not be protected against malware threats.

8.2. 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, click **Antivirus>Scan** in the settings console. The following window will appear:



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

8.2.1. 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. 52).

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 <code>Windows</code> , <code>Program Files</code> and <code>All Users</code> 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.



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.

8.2.2. 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.
- **Change Scan Target** - opens the **Properties** window, **Scan Path** tab, where you can change the scan target of the selected task.

**Note**

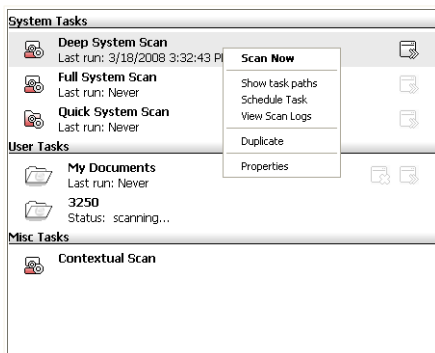
In the case of system tasks, this option is replaced by **Show Task Paths**, as you can only see their scan target.

- **Schedule Task** - opens the **Properties** window, **Scheduler** tab, where you can schedule the selected task.
- **View Scan Logs** - opens the **Properties** window, **Scan Logs** tab, where you can see the reports generated after the selected task was run.
- **Duplicate** - duplicates the selected task.

**Note**

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

- **Delete** - deletes the selected task.



Shortcut Menu

**Note**

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

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

**Note**

Due to the particular nature of the **Misc Tasks** category, only the **Properties** and **View Scan Logs** options are available in this case.

8.2.3. 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.

8.2.4. Configuring Scan Tasks

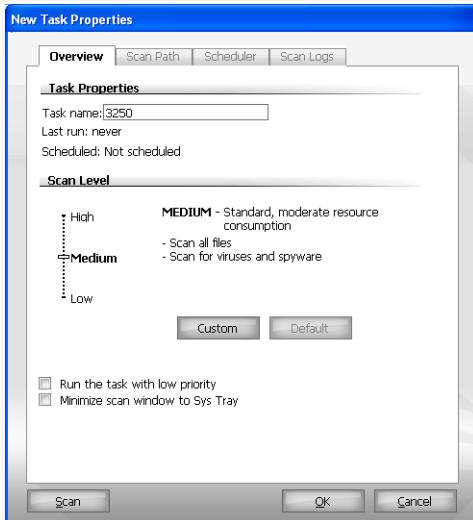
Each scan task has its own **Properties** window, where you can configure the scan options, set the scan target, schedule the task or see the reports. To open this window click the **Open** button, located on the right of the task (or right-click the task and then click **Open**).

**Note**

For more information on viewing logs and the **Logs** tab, please refer to "[Viewing Scan Logs](#)" (p. 70).

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

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.

<i>Protection level</i>	<i>Description</i>
	All files are scanned for viruses and spyware. Besides the classical signature-based scan, the heuristic analysis is also used.
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:

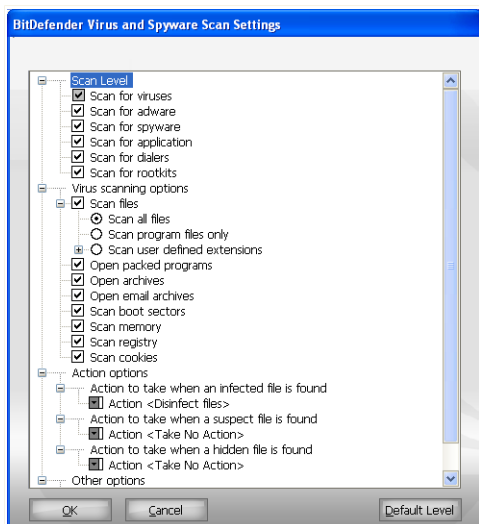
<i>Option</i>	<i>Description</i>
Run the task with Low priority	Decreases the priority of the scan process. You will allow other programs to run faster and increase the time needed for the scan process to finish.
Minimize scan window on start to systray	Minimizes the scan window to the system tray . Double-click the BitDefender icon to open it.

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 four categories:

- **Scan Level**
 - **Virus scanning options**
 - **Action options**
 - **Other options**
- Specify the type of malware you want BitDefender to scan for by selecting the appropriate options from the **Scan Level** category.

The following options are available:

<i>Option</i>	<i>Description</i>
Scan for viruses	Scans for known viruses.

<i>Option</i>	<i>Description</i>
	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.
Scan for spyware	Scans for known spyware threats. Detected files will be treated as infected.
Scan for application	Scans applications (.exe and .dll files).
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.

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

The following options are available:

<i>Option</i>	<i>Description</i>
Scan files	
Scan all files	All accessed files will be 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.

<i>Option</i>	<i>Description</i>
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.
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.

- Specify the actions to be taken on the infected, suspicious or hidden files detected in the **Action options** category. You can specify a different action for each category.
 - Select the action to be taken on the infected files detected. The following options are available:

<i>Action</i>	<i>Description</i>
None (log objects)	No action will be taken on infected files. These files will appear in the report file.
Disinfect files	Disinfects infected files.
Delete files	Deletes infected files immediately, without any warning.
Move files to Quarantine	Moves infected files into the quarantine.

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

<i>Action</i>	<i>Description</i>
None (log objects)	No action will be taken on suspicious files. These files will appear in the report file.

Action	Description
Delete files	Deletes suspicious files immediately, without any warning.
Move files to Quarantine	Moves suspicious files into the quarantine.

**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.
Make visible	Reveals hidden files so that you can see them.

**Note**

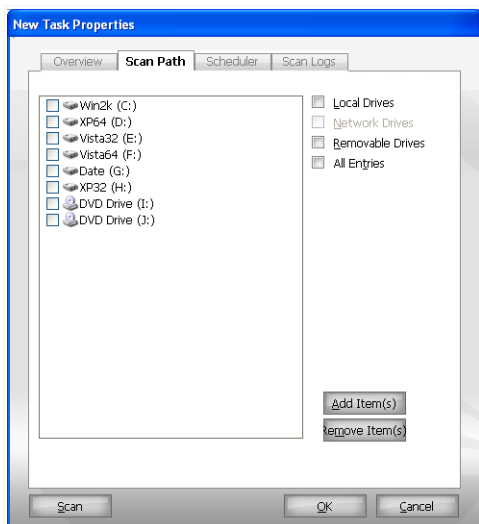
If you choose to ignore the detected files or if the chosen action fails, you will have to choose an action in the scanning wizard.

- To be prompted to submit all suspect files to the BitDefender lab after the scan process has finished, check **Submit suspect files to BitDefender Lab** in the **Other options** category.

If you click **Default** you will load the default settings. Click **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 **Change Scan Target**. The following window will appear:



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 Item(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

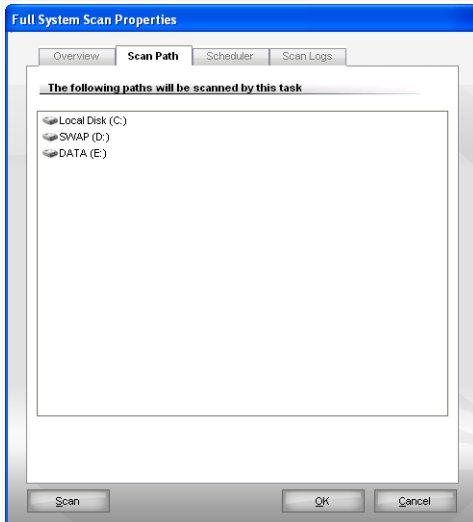
If you want to scan your entire computer, select the checkbox corresponding to **All Entries**.

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

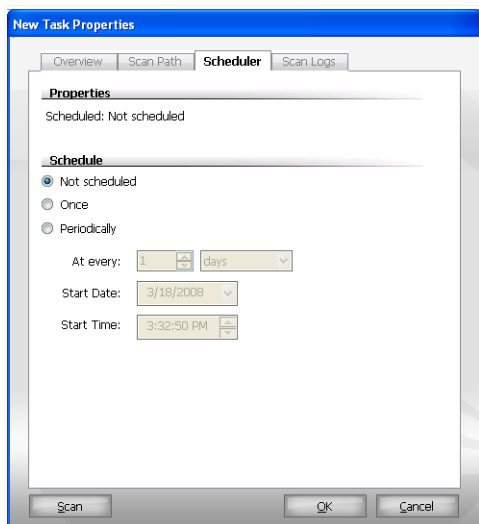
Full System Scan and **Deep System Scan** will scan all local drives, while **Quick System Scan** will only scan the `Windows` and `Program Files` folders.

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:



Scheduler

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.

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

8.2.5. 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 2008.
- **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.

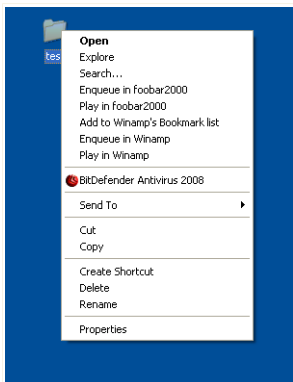
To run a scan task, use one of the following methods:

- 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. 65).

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.



Contextual Scan

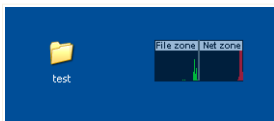
Right-click the file or folder you want to be scanned and select **BitDefender Antivirus 2008**.

The BitDefender Scanner will appear and the scanning will be initiated. For more information, please refer to "*BitDefender Scanner*" (p. 65).

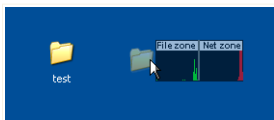
You can modify the scan options and see the report files by accessing the **Properties** window of the **Contextual Menu Scan** task.

Drag&Drop Scanning

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



Drag File



Drop File

The BitDefender Scanner will appear and the scanning will be initiated. For more information, please refer to "*BitDefender Scanner*" (p. 65).

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.

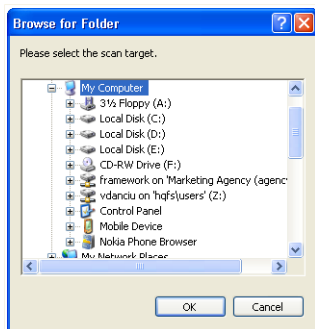


Note

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** → **Programs** → **BitDefender 2008** → **BitDefender Manual Scan**.

The following window will appear:



Manual Scanning

Choose the object that you want to be scanned and click **OK**.

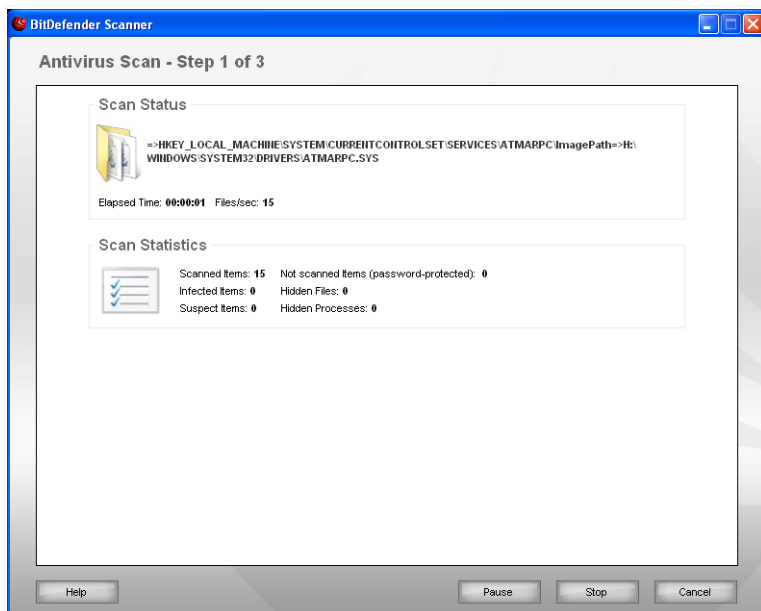
The BitDefender Scanner will appear and the scanning will be initiated. For more information, please refer to *"BitDefender Scanner"* (p. 65).

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.



Scanning

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.

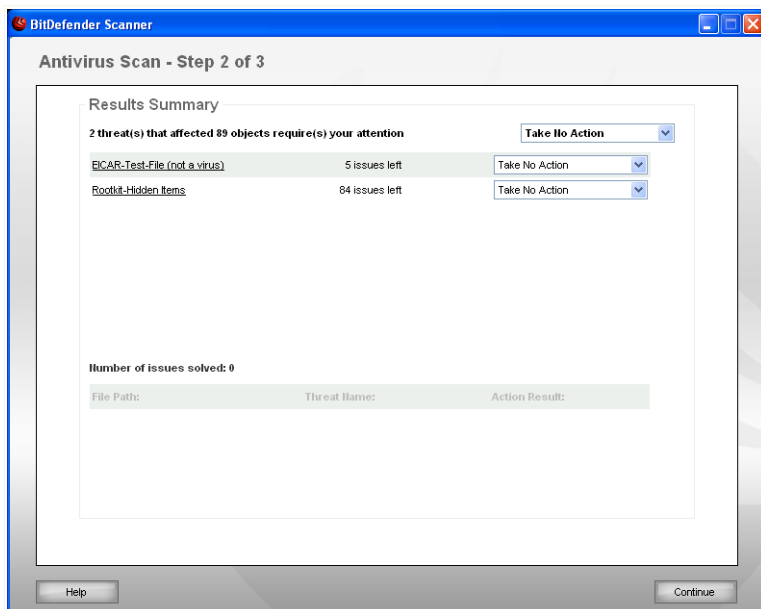
To temporarily stop the scanning process, just click **Pause**. You will have to click **Resume** to resume scanning.

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.



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 each group of issues or you can select separate actions for each issue.

The following options can appear on the menu:

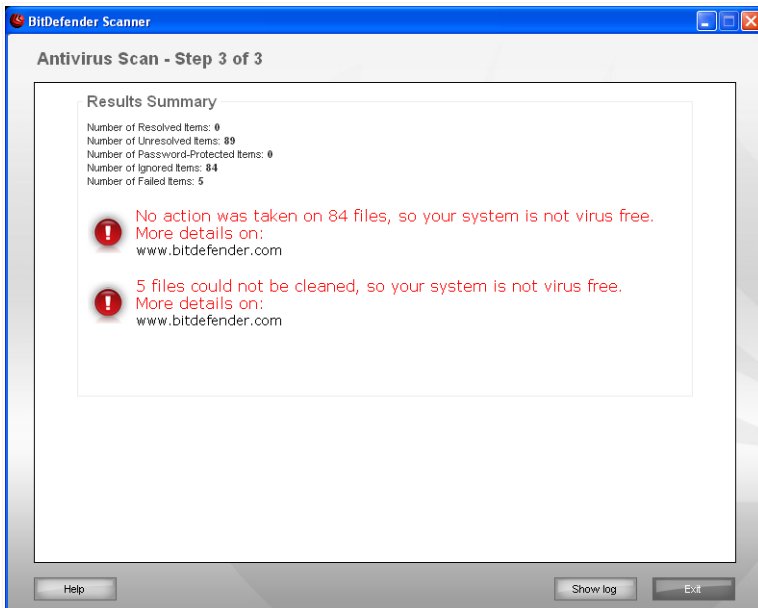
Action	Description
Take No Action	No action will be taken on the detected files.

Action	Description
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.



Summary

You can see the results summary. The report file is automatically saved in the **Logs** section from the **Properties** window of the respective task.



Important

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

Click **Exit** to close the results 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 Password-protected Items

The password-protected category includes two types of items: archives and installers. They do not present a real threat to the security of the system unless they contain infected files and only if executed.

To make sure that these items are clean:

- If the password-protected item is an archive you protected with a password, extract the files it contains and scan them separately. The easiest way to scan them is to right-click them and select **BitDefender Antivirus 2008** from the menu.
- If the password-protected item is an installer, make sure that **real-time protection** is enabled before you execute the installer. If the installer is infected, BitDefender will detect and isolate the infection.

If you do not want these objects to be detected again by BitDefender you must add them as exceptions to the scanning process. To add scan exceptions, click **Settings** to open the settings console and then go to **Antivirus > Exceptions**. For more information, please refer to **Objects Excluded from Scanning**.

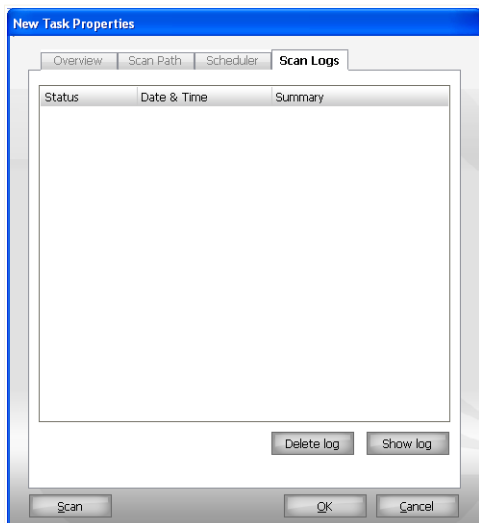
BitDefender Detected Suspect Files

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.

8.2.6. Viewing Scan Logs

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



Scan Logs

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



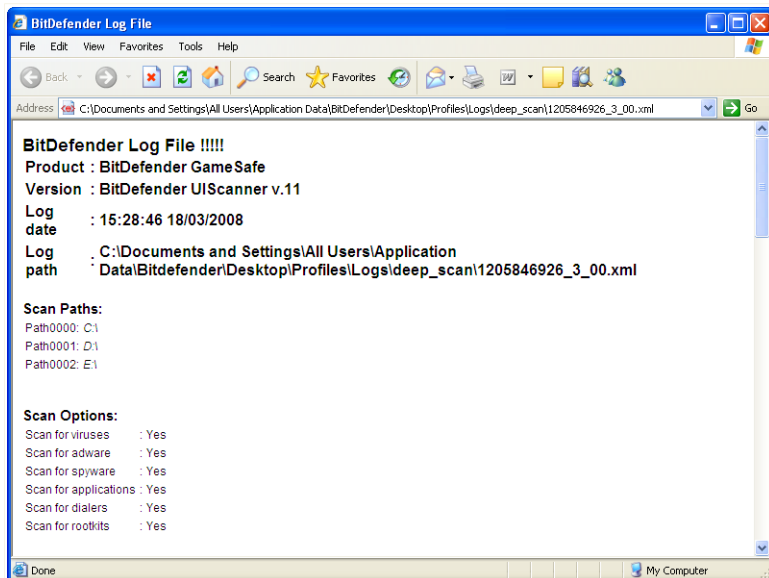
Note

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.

8.3. 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.

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.

**Note**

The exceptions specified here will NOT apply for contextual scanning.

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


To edit an entry from the table, select it and click the  **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**

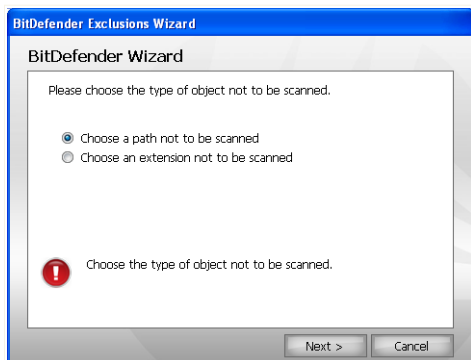
You can also right-click an object and use the options on the shortcut menu to edit or delete it.

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

8.3.1. 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.

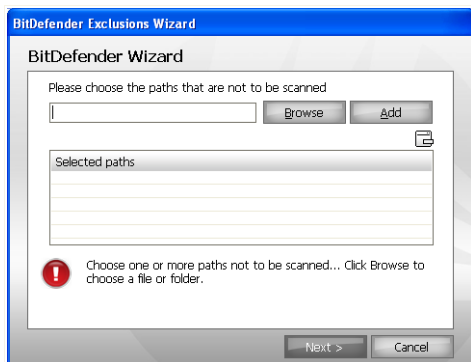
Step 1/3 - Select Object Type



Object Type

Select the option of excluding a path from scanning.
Click **Next**.

Step 2/3 - Specify Excluded Paths



Excluded Paths

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

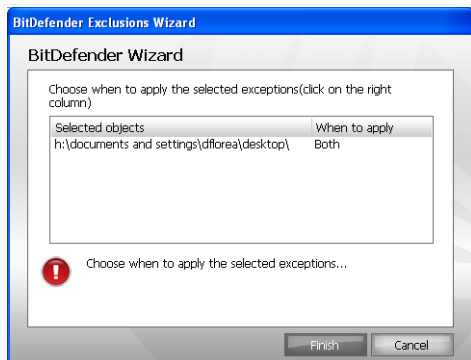
If the provided path does not exist, an error message will appear. Click **OK** and check the path for validity.

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  **Delete** button.

Click **Next**.

Step 3/3 - Select Scanning Type



Scanning Type


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.

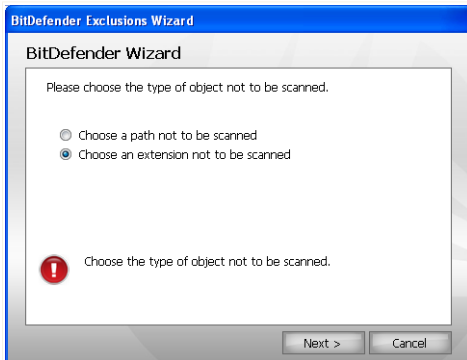
Click **Finish**.

Click **Apply** to save the changes.

8.3.2. 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 1/3 - Select Object Type

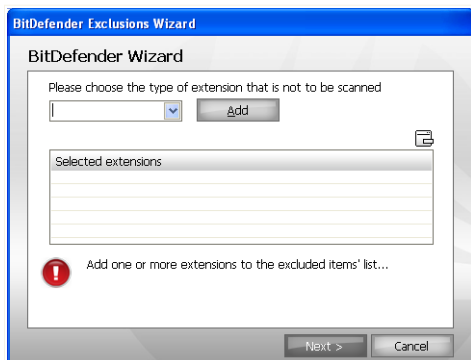


Object Type

Select the option of excluding an extension from scanning.

Click **Next**.

Step 2/3 - Specify Excluded Extensions



Excluded Extensions

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.

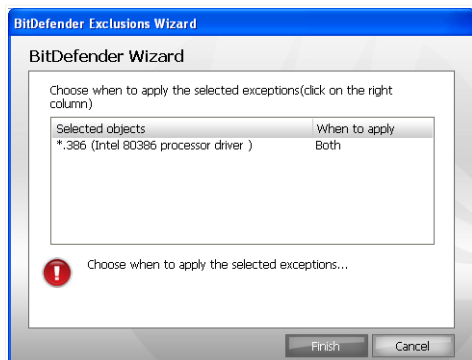
- Type the extension that you want to be excluded from scanning in the edit field and click **Add**.

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 3/3 - Select Scanning Type



Scanning Type

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.

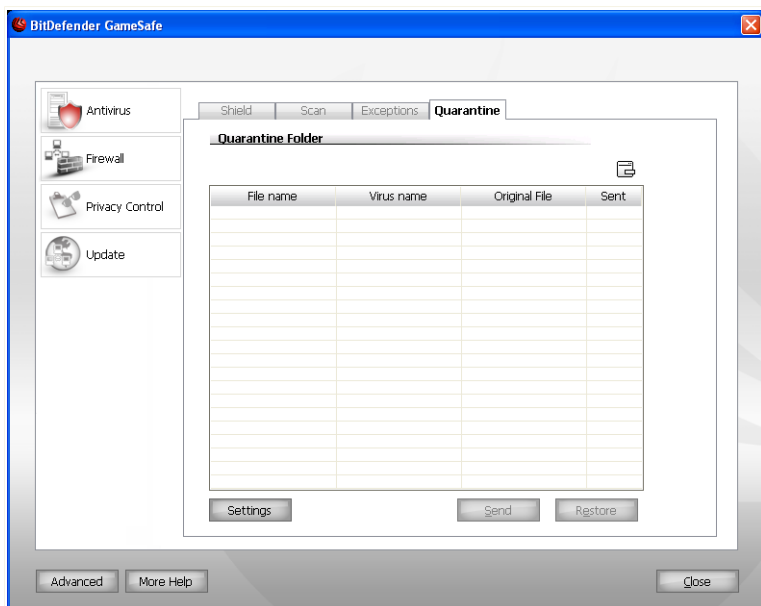
Click **Finish**.

Click **Apply** to save the changes.

8.4. 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, click **Antivirus>Quarantine** in the settings console.



Quarantine


8.4.1. Managing Quarantined Files

As you may notice, the **Quarantine** section contains a list of all the files that have been isolated so far. Every file has enclosed its name, the name of the detected virus, the path to its original location and the submission date.



Note

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

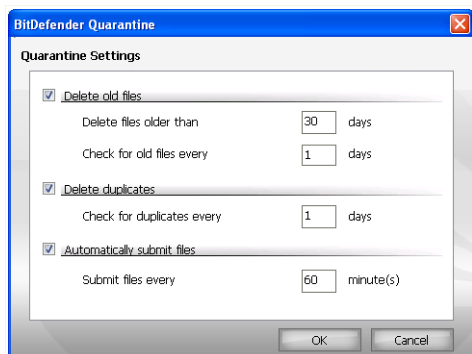
To delete a selected file from quarantine, click the  **Remove** button. If you want to restore a selected file to its original location, click **Restore**.

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

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.

8.4.2. Configuring Quarantine Settings

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



Quarantine Settings

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 10 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.

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

9. Firewall

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



Note

A firewall is essential if you have a broadband or DSL connection.

In Stealth Mode your computer is “hidden” from malicious software and hackers. The firewall module is capable of automatically detecting and protecting against port scans (streams of packets sent to a machine in order to find “access points”, often in preparation for an attack).

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

- [Firewall Insights](#)
- [Firewall Status](#)
- [Traffic Protection](#)
- [Advanced Settings](#)
- [Firewall Activity](#)
- [Network Zones](#)

9.1. Firewall Insights

The BitDefender Firewall was designed to offer the best protection for your network / Internet connections, without you having to configure it. No matter if you are connected directly to the Internet, to a single network or to several networks (Ethernet, wireless, VPN or other network type), either trusted or untrusted, the firewall will self-configure in order to adapt to the corresponding situation.

By default, BitDefender automatically detects the network configurations on your computer and it creates an appropriate basic firewall profile. It also adds detected networks to the profile as trusted or untrusted network zones, depending on their configuration.

9.1.1. What Are Firewall Profiles?

A firewall profile is a set of rules that controls applications' network / Internet access.

Depending on the network configuration on your computer, BitDefender automatically creates a specific type of profile. The basic profile created contains network access rules or elementary Internet access rules, required by system applications and BitDefender components.



Note

A single firewall profile is created, regardless of the number of networks you are connected to.

There are three types of basic profiles:

<i>Profile</i>	<i>Description</i>
Direct Connection	Contains the elementary Internet access rules recommended for a network configuration that allows direct access to Internet. The rules do not allow either network users to access your computer or you to browse the network.
Untrusted	Contains the network access rules recommended for a network configuration associated with an untrusted network. The rules allow you to browse the network, but prevent other network members from accessing your computer.
Trusted	Contains the network access rules recommended for a network configuration associated with a trusted network. No restrictions are imposed on network access. This implies that you have access to network shares, network printers and other network resources. At the same time, network members can connect to your computer and access your shares.

As applications try to connect to the Internet, appropriate rules are added to the profile. You can choose to allow or deny by default the access to Internet of applications for which rules have not been configured, or to allow only the whitelisted applications by default and to be asked permission for the other applications.



Note

To specify the access policy for applications that try to connect to the Internet for the first time, go to the **Status** section and set the protection level. To edit the existing profile, go to the **Traffic** section and click **Edit Profile**.

9.1.2. What Are Network Zones?

A network zone represents a computer inside a network or an entire network that is completely isolated from your computer or, on the contrary, that can detect your computer and connect to it. Practically, a zone is an IP address or a range of IP addresses that are allowed or denied access to your computer.

By default, BitDefender automatically adds zones for specific network configurations. A zone is added by creating an appropriate network access rule, applicable to an entire network, in the current profile.

There are two types of zones:

Zone Type	Description
Trusted zone	<p>Computers from a trusted zone can connect to your computer and you can connect to them.</p> <p>All connection attempts coming from such a zone, as well as all connection attempts from your computer to such a zone are allowed. If a network is added as a trusted zone, you have unrestricted access to network shares, network printers and other network resources. Also, network members can connect to your computer and access your shares.</p>
Untrusted zone	<p>Computers from an untrusted zone cannot connect to your computer and you cannot connect to them either.</p> <p>All connection attempts coming from such a zone, as well as all connection attempts from your computer to such a zone are blocked. As the ICMP traffic is denied and the Stealth Mode is enabled, your computer is practically invisible for computers in that zone.</p>



Note

To edit a zone, go to the **Zones** section. To edit the rule corresponding to a zone, go to the **Traffic** section and click **Edit Profile**.

9.1.3. Firewall Operation

When rebooting the system after installation, BitDefender automatically detects your network configuration, creates an appropriate basic profile and adds a zone depending on the detected network.



Note

If you connect directly to the Internet, no network zone is created for the corresponding network configuration. If you are connected to more than one network, zones are added depending on the respective networks.

Each time the network configuration changes, whether you connect to another network or you disable a network connection, a new firewall profile is created. At the same time, the network zones are modified accordingly.

When a new firewall profile is created, the old profile is saved, so that it can be reloaded when you go back to its corresponding network configuration.

Depending on the network configuration, BitDefender will configure itself accordingly. This is how the BitDefender Firewall is configured by default:

- If you connect directly to Internet, no matter if you are also connected to other networks, a Direct Connection profile is created. Otherwise, BitDefender creates an untrusted firewall profile.



Note

As a matter of security, trusted profiles are not created by default. To create a trusted profile, you must reset the existing profile. For more information, please refer to [“Resetting Profiles” \(p. 97\)](#).

- Zones are added depending on the network configuration.

Zone Type	Network Configuration
Trusted zone	Private IP with no gateway - The computer is part of a local area network (LAN) and does not connect to the Internet. An example of such situation is a home network created to allow family members to share files, printers or other resources.
	Private IP with Domain Controller detected - The computer is part of a LAN and connected to a domain. An example of such situation is an office network that allows users to share

Zone Type	Network Configuration
	files or other resources inside a domain. A domain implies the existence of a set of policies with which member computers comply.
Untrusted zone	Open (not secured) wireless - The computer is part of a wireless local area network (WLAN). An example of such situation is when you access the Internet using a free access point from a public place.

**Note**

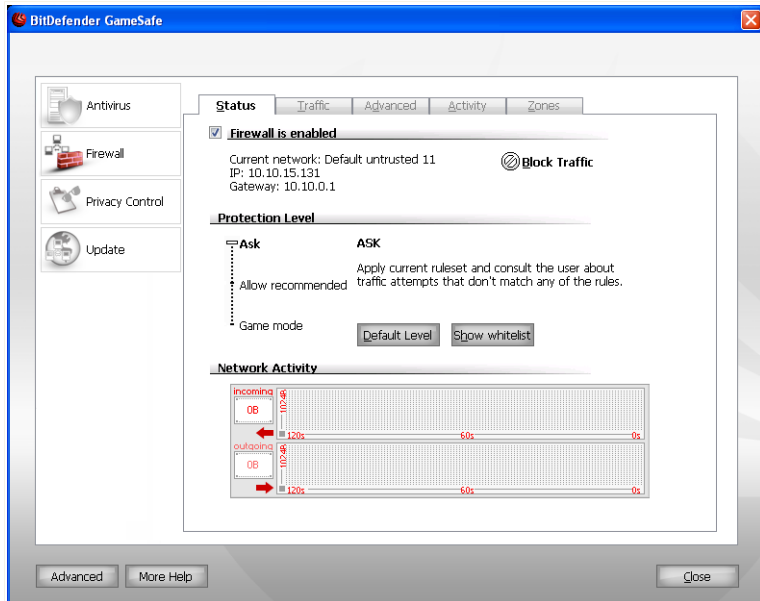
Zones are not created for some network configurations, such as:

- **Public (routable) IP** - The computer is directly connected to Internet.
- **Private IP with gateway, but no Domain Controller detected** - The computer is part of a LAN, without being part of a domain too, and it connects to Internet through a gateway. An example of such situation is a school campus network that allows users to share files or other resources.

- Stealth Mode is enabled.
- VPN and Remote connection are allowed.
- Internet Connection Sharing is not allowed for untrusted zones.
- Whitelisted applications are automatically allowed access, whereas for the other applications you will be asked for permission the first time they try to connect.

9.2. Firewall Status

To configure the firewall protection, click **Firewall>Status** in the settings console. The following window will appear:



Firewall Status


In this section you can enable/disable the **Firewall**, block all network/internet traffic and set the default behaviour on new events.



Important

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

To block all network / Internet traffic click  **Block Traffic** and then **Yes** to confirm your choice. This will isolate your computer from any other computer in the network.

To unblock the traffic later, just click  **Unblock Traffic**.

At the bottom of the section you can see the BitDefender statistics regarding incoming and outgoing traffic. The graph shows the internet traffic volume over the last two minutes.



Note

The graph appears even if the **Firewall** is disabled.

9.2.1. 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.

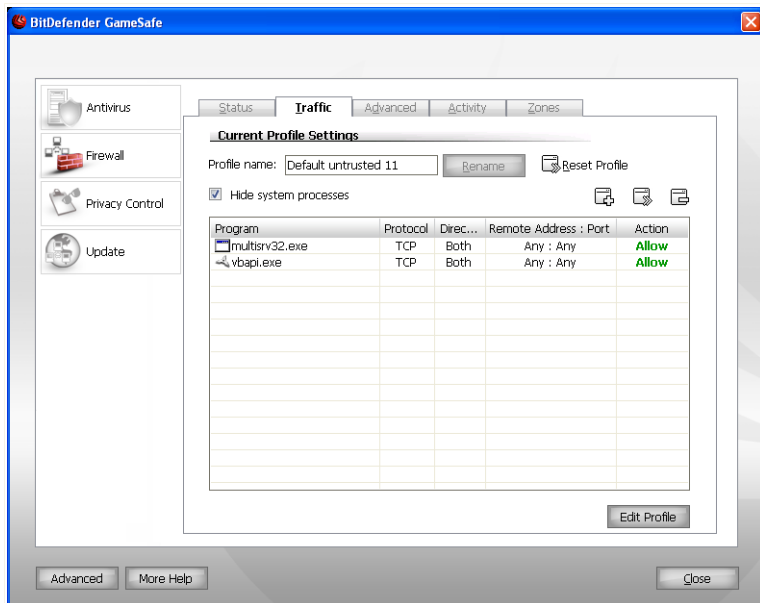
There are 3 protection levels:

Protection level	Description
Game Mode	Applies the current rules and allows all traffic attempts that do not match any of the current rules without prompting. This policy is strongly discouraged, but it might be useful for network administrators and gamers.
Allow recommended	Applies the current rules and allows all outgoing connection attempts from programs which are known to be legitimate (whitelisted) by BitDefender without prompting. For the rest of connection attempts, BitDefender will ask for your permission. You can see the traffic rules as they are created in the Traffic section. Whitelisted programs are the most commonly used applications worldwide. They include the most known web browsers, audio&video players, chat and filesharing programs, as well as server clients and operating system applications. If you want to see which programs are whitelisted, click Show Whitelist .
Ask	Applies the current rules and consults you about all traffic attempts that do not match any of the current rules.

Click **Default Level** to set the default policy (**Allow recommended**).


9.3. Traffic Control

To manage the firewall rules of the current profile, click **Firewall>Traffic** in the settings console. The following window will appear:



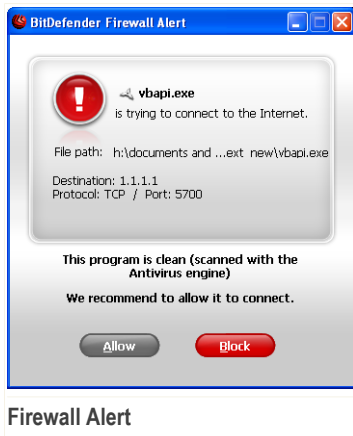
Traffic Control

In this section you can specify which incoming or outgoing connections to permit/deny by creating rules with specific protocols, ports, applications and/or remote addresses.

The rules can be input automatically (through the alert window) or **manually** (click the  **Add** button and choose the parameters for the rule).

9.3.1. Adding Rules Automatically

With **Firewall** enabled, BitDefender will ask for your permission whenever a connection to the Internet has been made:



You can see the following: the application that is trying to access the Internet, the path to the application file, the destination, the protocol used and the **port** on which the application is trying to connect.

Click **Allow** to allow all traffic (inbound and outbound) generated by this application from the local host to any destination, over the respective IP protocol and on all ports. If you click **Block**, the application will be denied access to the Internet over the respective IP protocol completely.


Based on your answer, a rule will be created, applied and listed in the table. The next time the application tries to connect, this rule will be applied by default.

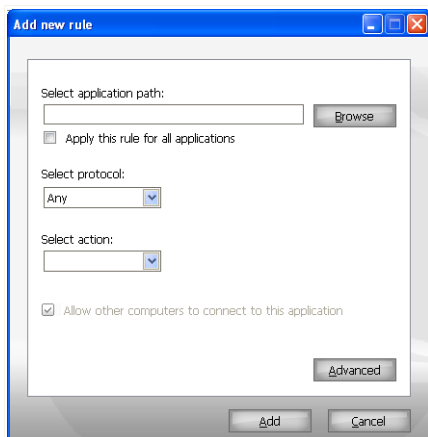


Important

Allow inbound connection attempts only from IPs or domains you are sure to trust.

9.3.2. Adding Rules Manually

Click the  **Add rule** button and choose the parameters of the rule. The following window will appear:



Add Rule

To add a new firewall rule, follow these steps:

1. Select the application for which the new firewall rule will be created.

To select an application, click **Browse**, locate it and click **OK**.

If you want to create a rule for all applications, just check **Apply this rule for all applications**.

2. Select the protocol to which the rule will apply.

A list with the most common protocols is available to help you select only specific protocol. Select the desired protocol (on which the rule applies) from the corresponding drop-down menu or select **Any** to select all the protocols.

The following table lists the protocols you can select along with a short description of each:

Protocol	Description
ICMP	Internet Control Message Protocol - is an extension to the Internet Protocol (IP). ICMP supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

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

3. Select the rule action from the corresponding menu.

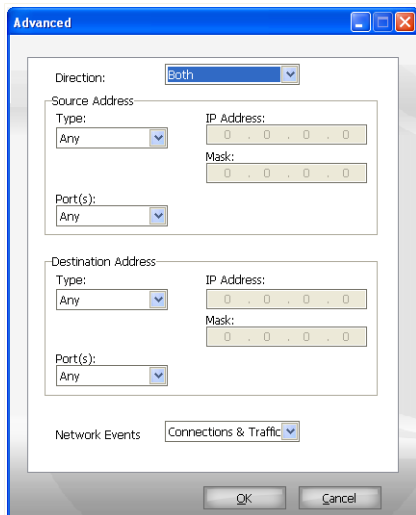
Action	Description
Allow	The specified application will be allowed network / Internet access under the specified circumstances.
Deny	The specified application will be denied network / Internet access under the specified circumstances.

4. If the previously selected protocol is TCP or UDP, you can specify whether the rule will apply to the application when it acts as a server or not.

Check **Allow other computers to connect to this application** to apply the action to all network events. Implicitly, you will allow or deny this application's right to open ports.

If you want to apply the action only to traffic for UDP and traffic & connections for TCP respectively, clear the corresponding check box.

If you want to configure more advanced settings for the rule, click **Advanced**. A new window will appear:



Advanced Rule Settings

You can configure the following:

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

<i>Type</i>	<i>Description</i>
Outbound	The rule applies only for the outgoing traffic.
Inbound	The rule applies only for the incoming traffic.
Both	The rule applies in both directions.

- **Source Address** - specify the source address.

To specify the source address, select the address type from the menu and specify the required data. The following options are available:

<i>Type</i>	<i>Description</i>
Any	The rule applies to any source address.

<i>Type</i>	<i>Description</i>
Host	The rule applies only if the source is a specific host. You must type in the IP address of the host.
Network	The rule applies only if the source is a specific network. You must type in the IP address and the mask of the network.
Local Host	The rule applies only if the source is the local host. If you use more than one network interface, select from the menu the network interface to which the rule applies. If you want the rule to apply to all local hosts, select Any .
Local Network	The rule applies only if the source is the local network. If you are connected to more than one network, select from the menu the network to which the rule applies. If you want the rule to apply to all local networks, select Any .

If you have selected TCP or UDP as protocol you can set a specific port or a range between 0 and 65535. If you want the rule to apply to all ports, select **Any**.

- **Destination Address** - specify the destination address.

To specify the destination address, select the address type from the menu and specify the required data. The following options are available:

<i>Type</i>	<i>Description</i>
Any	The rule applies to any destination address.
Host	The rule applies only if the destination is a specific host. You must type in the IP address of the host.
Network	The rule applies only if the destination is a specific network. You must type in the IP address and the mask of the network.
Local Host	The rule applies only if the destination is the local host. If you use more than one network interface, select from the menu the network interface to which the rule applies. If you want the rule to apply to all local hosts, select Any .
Local Network	The rule applies only if the destination is the local network. If you are connected to more than one network, select from the menu the network to which the rule applies. If you want the rule to apply to all local networks, select Any .

If you have selected TCP or UDP as protocol you can set a specific port or a range between 0 and 65535. If you want the rule to apply to all ports, select **Any**.

- **Network Events** - if you have selected TCP or UDP as protocol, choose the network events to which the rule applies.

Click **OK** to close the advanced settings window.

Click **Add** to add the firewall rule.

9.3.3. Managing Rules

You can see the rules created so far for the current profile in the table.

Select the check box corresponding to **Hide system processes** to hide the rules regarding the system or the BitDefender processes.

Rules are listed by order of priority starting from the top, with the first rule counting as the highest priority. Click **Edit profile** to enter the **Detailed view** display where you can change the priority of the rules by moving them up and down.

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

To modify a rule select it and click the  **Edit rule** button or double-click the rule.

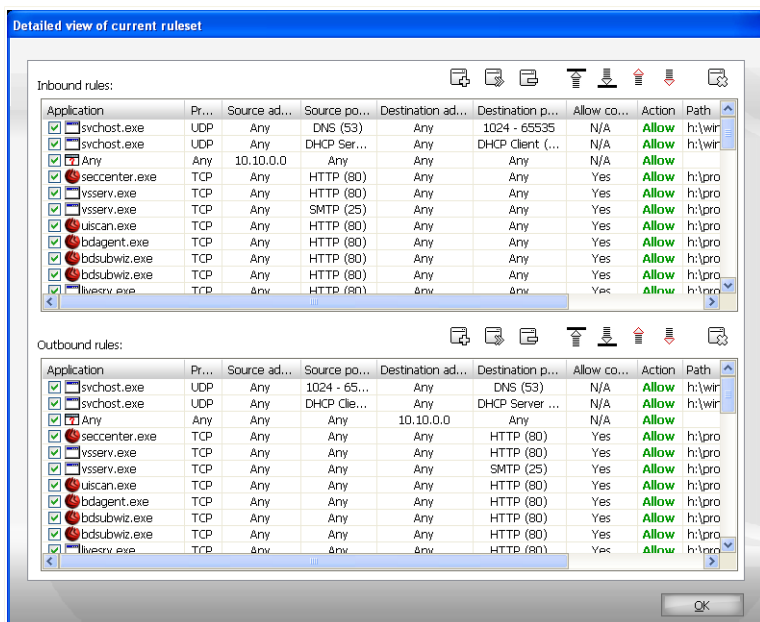


Note

A contextual menu is also available and it contains the following options: **Add rule**, **Delete rule** and **Edit rule**.

9.3.4. Modifying Profiles

You can modify a profile by clicking **Edit profile**. The following window will appear:



Detailed View

Rules are divided into 2 sections: inbound rules and outbound rules. You can see the application and the rule parameters of each rule (source address, destination address, source ports, destination port, action, etc).

To delete a rule, just select it and click the **Delete rule** button. To delete all the rules click the **Clear list** button. To modify a rule, either select it and click the **Edit rule** button or double-click it. To temporarily deactivate a rule without deleting it, clear the corresponding check box.

You can increase or decrease the priority of a rule. Click the **Move Up In List** button to increase the priority of the selected rule by one level, or click the **Move Down In List** button to decrease the priority of the selected rule by one level. To assign a rule the highest priority, click the **Move First** button. To assign a rule the lowest priority, click the **Move Last** button.

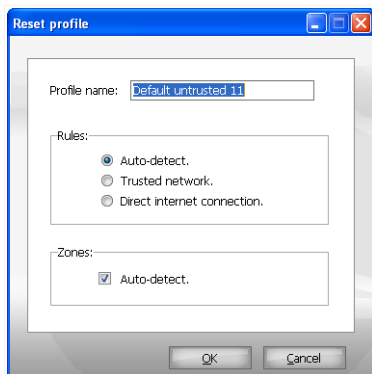
**Note**

A contextual menu is also available and it contains the following options: **Add rule**, **Edit rule**, **Delete rule**, **Move up**, **Move down**, **Move first**, **Move last** and **Clear list**.

Click **OK** to close the window.

9.3.5. Resetting Profiles

Advanced users may choose to reconfigure the firewall profile in order to optimize the firewall protection or to customize it according to their needs. To reset the firewall profile, click **Reset Profile**. The following window will appear:



Reset Profile

You can configure the following:

- **Profile name** - type a new name in the edit field.
- **Rules** - specify what type of rules should be created for system applications.

The following options are available:

<i>Option</i>	<i>Description</i>
Auto-detect	Lets BitDefender detect the network configuration and create an appropriate set of elementary rules.
Trusted network	Creates a set of elementary rules appropriate for a trusted network.

<i>Option</i>	<i>Description</i>
Direct Internet connection	Creates a set of elementary rules appropriate for a direct connection to Internet.

- **Zones** - check **Auto-detect** to let BitDefender create appropriate zones for the detected networks.

Click **OK** to close the window and reset the profile.

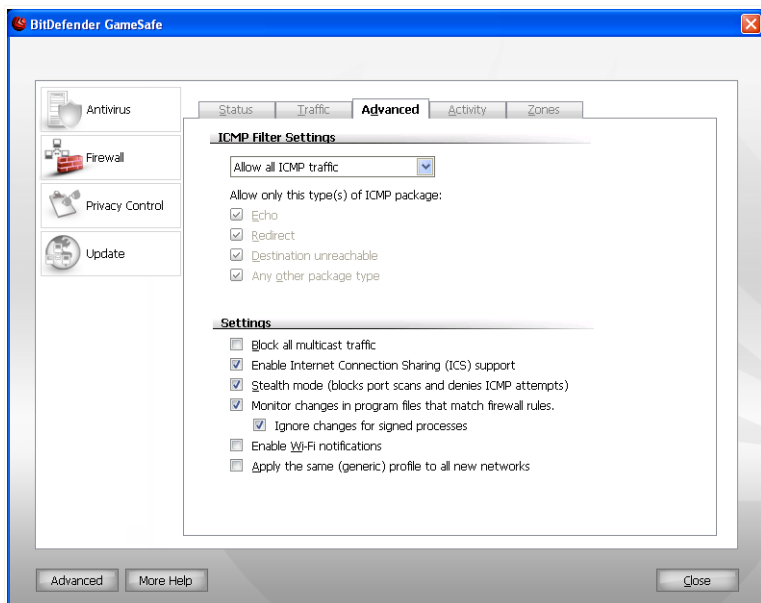


Important

All the rules that you added in this section will be lost if you choose to reconfigure the firewall profile.

9.4. Advanced Settings

To configure the advanced settings of the BitDefender firewall, click **Firewall>Advanced** in the settings console. The following window will appear:



Advanced Settings

In this section you can configure the advanced settings of the BitDefender firewall. The advanced settings allow you to specify the filtering rules for the ICMP traffic (**ICMP Settings**) and to block multicast traffic, to share your Internet connection or make your computer invisible to malicious software and hackers (**Settings**).

9.4.1. Configuring ICMP Filtering Settings

From the menu, you can select one of the following policies to filter the ICMP traffic:

- **Allow all ICMP traffic** - allows all the ICMP traffic.
- **Block all ICMP traffic** - blocks all the ICMP traffic.
- **Custom ICMP filtering** - customizes the way ICMP traffic is filtered. You will be able to choose what types of ICMP packages to allow.

The following options are available:

Option	Description
Echo	This option enables the Echo Reply and Echo Request messages. The Echo Request is an ICMP message which sends a packet of data to the host and expects that data to be sent in return in a Echo Reply. The host must respond to all Echo Requests with an Echo Reply containing the exact data received in the request message. The Echo Reply is an ICMP message generated in response to an ICMP Echo Request message, and is mandatory for all hosts and routers.
Redirect	This is an ICMP message which informs a host to redirect its routing information (to send packets on an alternate route). If the host tries to send data through a router (R1) and then another router (R2) to reach the host, and a direct path from the host to R2 is available, the redirect will inform the host of such a route. The router will still send the original datagram to the intended destination. However, if the datagram contains routing information, this message will not be sent even if a better route is available.
Destination unreachable	This is an ICMP message which is generated by the router to inform the client that the destination host is unreachable, unless the datagram has a multicast address. Reasons for this message may include the physical connection to the host does not exist (distance is infinite), the indicated protocol or port is not active, or the data must be fragmented but the 'don't fragment' flag is on.
Any other package type	With this option enabled any other package than Echo , Destination unreachable or Redirect will pass.

9.4.2. Configuring Advanced Firewall Settings

The following advanced firewall settings are available:

- **Block all multicast traffic** - drops any multicast package received.

Multicast traffic is the kind of traffic addressing a special group in a network. Packages are sent to a special address from where the multicast client can receive them if he agrees to.

For example, a member of a network who owns a TV-tuner may broadcast (send to each network member) or multicast (send to a special address) the video stream. The computers that listen the multicast address can accept or reject the package. If accepted, the video stream can be watched by the multicast clients.

Excessive amounts of multicast traffic consumes bandwidth and resources. With this option enabled, any multicast package received will be dropped. However, it is not recommended to select this option.

- **Enable Internet Connection Sharing(ICS) support** - enables support for Internet Connection Sharing(ICS).



Note

This option does not automatically enable ICS on your system, but only allows this type of connection in case you enable it from your operating system.

Internet Connection Sharing (ICS) enables members of local area networks to connect to the Internet through your computer. This is useful when you benefit from a special/particular Internet connection (e.g. wireless connection) and you want to share it with other members of your network.

Sharing your Internet connection with members of local area networks leads to a higher resource consumption level and may involve a certain risk. It also takes off some of your ports (those opened by the members who are using your Internet connection).

- **Stealth Mode** - makes your computer invisible to malicious software and hackers.

A simple way of finding out whether your computer might be vulnerable is to connect to ports to see if there is any response. This is called a port scan.

Malicious individuals or software programs need not find out that your computer even exists, let alone provides services to the network. The **Stealth Mode** option will stop your machine from responding to attempts to find out which ports are open, or where exactly it is.

- **Monitor changes in program files that match firewall rules** - checks each application attempting to connect to the Internet to see if it has been changed since the rule controlling its access was added. If the application has been changed, an alert will prompt you to allow or to block the access of the application to the Internet.

Usually, applications are changed by updates. But, there is a risk that they might be changed by malware applications, with the purpose of infecting your computer and other computers in the network.



Note

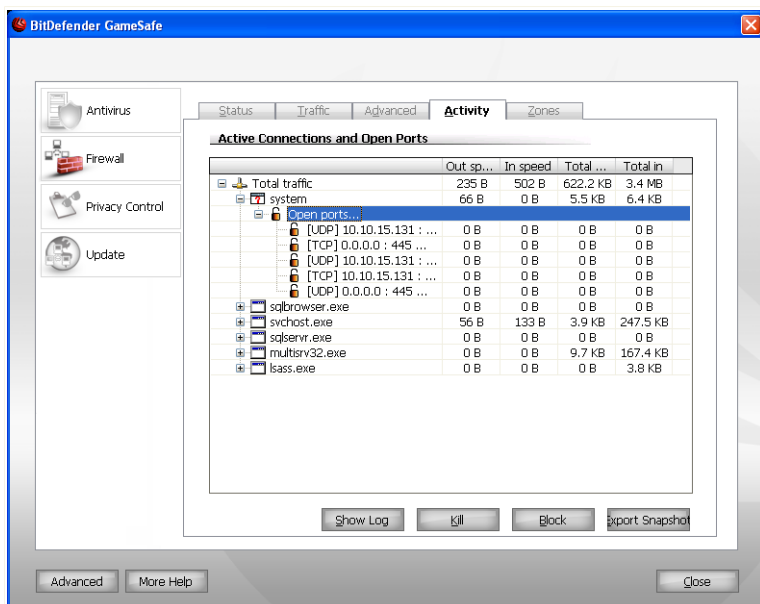
We recommend you to keep this option selected and to allow access only to those applications that you expect to have changed after the rule controlling their access was created.

Signed applications are supposed to be trusted and have a higher degree of security. You can check **Ignore changes for signed processes** in order to allow changed signed applications to connect to the Internet without your receiving an alert about this event.

- **Enable Wi-Fi notifications** - enables the Wi-Fi notifications.
- **Apply the same (generic) profile to all new networks** - creates a default (generic) **firewall profile**, named `Generic Network`, and applies it whenever a new network configuration is detected. If you go back to an old network configuration for which a firewall profile exists, the respective firewall profile is loaded instead of the generic profile.

9.5. Connection Control

To monitor the current network / Internet activity (over TCP and UDP) sorted by application and to open the BitDefender Firewall log, click **Firewall>Activity** in the settings console. The following window will appear:



Connection Control

You can see the total traffic sorted by application. For each application, you can see the connections and the open ports, as well as statistics regarding the outgoing & incoming traffic speed and the total amount of data sent / received.

The window presents the current network / Internet activity in real-time. As connections or ports are closed, you can see that the corresponding statistics are dimmed and that, eventually, they disappear. The same thing happens to all statistics corresponding to an application which generates traffic or has open ports and which you close.

Click **Block** to create rules that restrict traffic by the selected application, port or connection. You will be requested to confirm your choice. The rules can be accessed in the **Traffic** section for further fine-tuning.



Note

To block an application, port or connection, you can also right-click it and select **Block**.

Click **Kill** to end all instances of a selected process. You will be requested to confirm your choice.



Note

To kill a process, you can also right-click it and select **Kill**.

Click **Export Snapshot** to export the list to a `.txt` file.

For a comprehensive list of events regarding the Firewall module usage (starting/stopping firewall, traffic blocking, enabling Stealth Mode, modifying settings, applying a profile) or generated by the activities detected by it (scanning ports, blocking connection attempts or traffic according to the rules) check the BitDefender Firewall log file that can be viewed by clicking **Show Log**. The file is located in the Common Files folder of the current Windows user, under the path:
`...BitDefender\BitDefender Firewall\bdfirewall.txt`.

9.6. Network Zones

A zone is an IP address or a range of IP addresses for which a special rule is created inside a profile. The rule can either allow network members unrestricted access to your computer (trusted zones) or, on the contrary, completely isolate your computer from network computers (untrusted zone).

By default, BitDefender automatically detects the network you are connected to and adds a zone depending on the network configuration.



Note

If you are connected to several networks, depending on their configuration, more than one zone may be added.

Trusted zones are added by default for the following network configurations:

- **Private IP with no gateway** - The computer is part of a local area network (LAN) and it does not connect to the Internet.
- **Private IP with Domain Controller detected** - The computer is part of a LAN and connected to a domain.

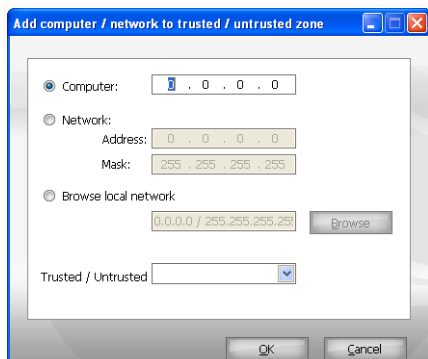
Untrusted zones are added by default for the following network configurations:

- **Open (not secured) wireless** - The computer is part of a wireless local area network (WLAN).

9.6.1. Adding Zones

You can add zones manually. This allows you, for example, to share files only with your friends inside an open wireless network (by adding their computers as trusted zones), or to block a computer from a trusted network (by adding it as an untrusted zone).

To add a new zone, click the  **Add Zone** button. The following window will appear:



Add Zone

To add a zone, follow these steps:

1. Specify a computer from a local network or an entire local network that you want to be added as a zone. You can use one of the following methods:
 - To add a specific computer, select **Computer** and provide its IP address.
 - To add a specific network, select **Network** and provide its IP address and mask.
 - Browse the local networks to find and add a computer or a network.

To browse the local networks, select **Browse local network** and then click **Browse**. A new window will appear where you can see all the networks you are connected to as well as all members of each network.

Select from the list the computer or the network that you want to be added as a zone and click **OK**

2. Select from the menu what kind of zone you want to create (trusted or untrusted).
3. Click **OK** to add the zone.

10. 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.

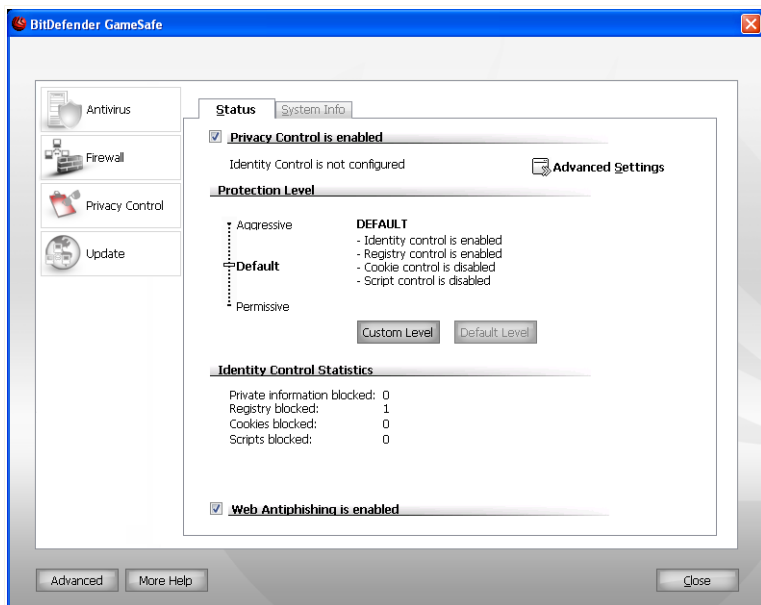
BitDefender also scans the web sites you visit and alerts you if any phishing threat is detected.

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

- [Privacy Control Status](#)
- [Advanced Settings - Identity Control](#)
- [Advanced Settings - Registry Control](#)
- [Advanced Settings - Cookie Control](#)
- [Advanced Settings - Script Control](#)
- [System Information](#)
- [Antiphishing Toolbar](#)

10.1. Privacy Control Status

To configure the Privacy Control and to view information regarding its activity, click **Privacy Control>Status** in the settings console. The following window will appear:



Privacy Control Status

10.1.1. Privacy Control



Important

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

The Privacy Control protects your computer using 5 important protection controls:

- **Identity Control** - protects your confidential data by filtering all outgoing HTTP and SMTP traffic according to the rules you create in the **Identity** section.



Note

At the bottom of the section you can see the **Identity Control statistics**.

- **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.

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

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:

<i>Protection level</i>	<i>Description</i>
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.

10.1.2. Antiphishing Protection

Phishing is a criminal activity on the Internet that uses social engineering techniques in order to trick people into giving away private information.

Most of the times, phishing attempts come down to sending mass e-mail messages which falsely claim to come from an established, legitimate enterprise. These spoofed messages are sent in the hope that at least a few of the receivers that match the profile of the phishing target will be persuaded to divulge private information.

A phishing message usually presents an issue related to your online account. It tries to convince you to click a link provided within the message to access a supposedly legitimate web site (in fact, a forged one) where private information is requested. You may be asked, for example, to confirm account information, such as username and password, and to provide your bank account or social security number. Sometimes,

to be more convincing, the message may pretend that your account has already been or is threatened to be suspended if you do not use the link provided.

Phishing also makes use of spyware, such as Trojan keyloggers, to steal account information directly from your computer.

The main phishing targets are customers of online payment services, such as eBay and PayPal, as well as banks that offer online services. Recently, users of social networking websites have also been targeted by phishing in order to obtain personal identification data used for identity theft.

To be protected against phishing attempts when you are surfing the Internet, keep **Antiphishing** enabled. In this way, BitDefender will scan each web site before you access it and it will alert you of the existence of any phishing threat. A White List of web sites that will not be scanned by BitDefender can be configured.

In order to easily manage antiphishing protection and the White List, use the BitDefender Antiphishing toolbar integrated into Internet Explorer. For more information, please refer to "*Antiphishing Toolbar*" (p. 126).

10.2. Advanced Settings - 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.

Identity Control helps you keep confidential data safe. It scans the HTTP or SMTP traffic, or both, for certain strings that you have defined. If a match is found, the respective web page or e-mail is blocked.

Multiuser support is provided so that no other user of the system can see the rules you have configured.

The privacy rules can be configured in the **Identity** section. To access this section, open the **Advanced Privacy Control Settings** window and click the **Identity** tab.



Note

To open the **Advanced Privacy Control Settings** window, click **Privacy Control>Status** in the settings console and click  **Advanced Settings**.

Step 1/3 - Set Rule Type and Data

Set Rule Type and Data

Enter the name of the rule in the edit field.

You must set the following parameters:

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



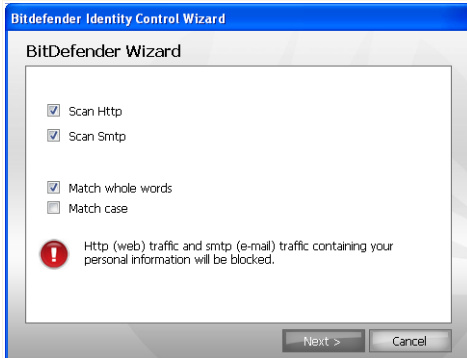
Note

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.

Click **Next**.

Step 2/3 - Select Traffic



Select Traffic

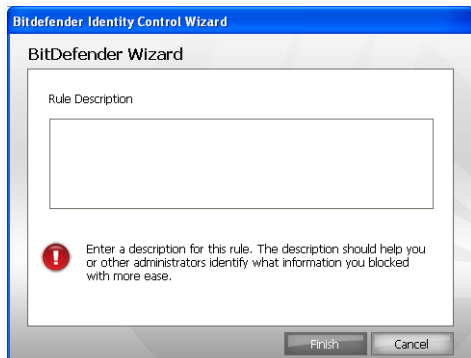
Select the type of traffic you want BitDefender to scan. The following options are available:

- **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.

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.

Click **Next**.

Step 3/3 - Describe Rule



Describe Rule

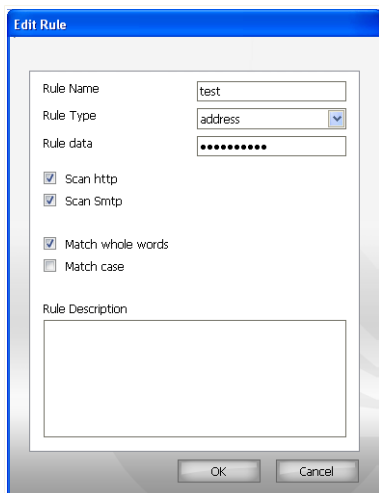
Enter a short description of the rule in the edit field.

Click **Finish**.

10.2.2. 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**.



Edit Rule

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

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

10.3. Advanced Settings - Registry Control

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

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

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



Registry Alert

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

If you want BitDefender to remember your answer, check **Always apply this action to this program**. In this way, a rule will be created and the same action will be applied whenever this program tries to modify a registry entry in order to be executed at Windows start-up.

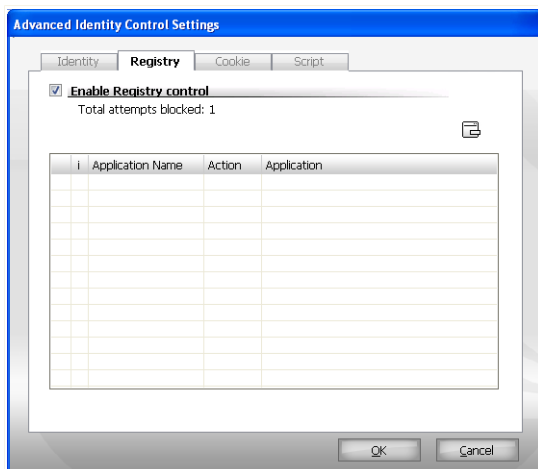
**Note**

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

Every rule that has been remembered can be accessed in the **Registry** section for further fine-tuning. To access this section, open the **Advanced Privacy Control Settings** window and click the **Registry** tab.


**Note**

To open the **Advanced Privacy Control Settings** window, click **Privacy Control>Status** in the settings console and click  **Advanced Settings**.



Registry Control

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

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

To change the action of a rule, double-click the action field and select the appropriate option from the menu.

Click **OK** to close the window.

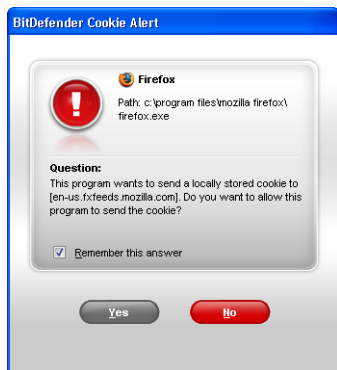
10.4. Advanced Settings - Cookie Control

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:



Cookie Alert

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

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

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



Note

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

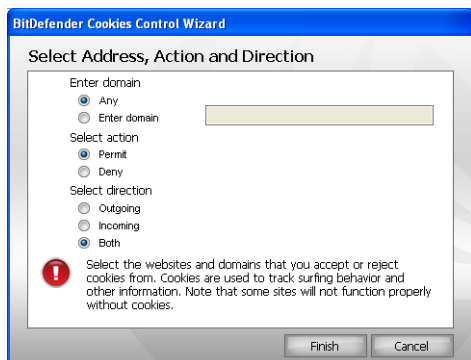
Every rule that has been remembered can be accessed in the **Cookie** section for further fine-tuning. To access this section, open the **Advanced Privacy Control Settings** window and click the **Cookie** tab.



Note

To open the **Advanced Privacy Control Settings** window, click **Privacy Control**>**Status** in the settings console and click  **Advanced Settings**.

Step 1/1 - Select Address, Action and Direction



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.

<i>Action</i>	<i>Description</i>
Permit	The cookies on that domain will execute.
Deny	The cookies on that domain will not execute.

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

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

Click **Finish**.

**Note**

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

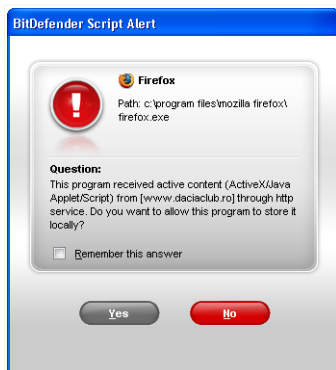
Click **OK** to save the changes and close the window.

10.5. Advanced Settings - Script Control

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

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

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



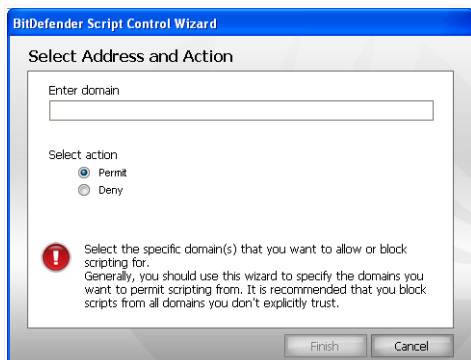
Script Alert

You can see the name of the resource.

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

Every rule that has been remembered can be accessed in the **Script** section for further fine-tuning. To access this section, open the **Advanced Privacy Control Settings** window and click the **Script** tab.

Step 1/1 - Select Address and Action



Select Address and Action

You can set the parameters:

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

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

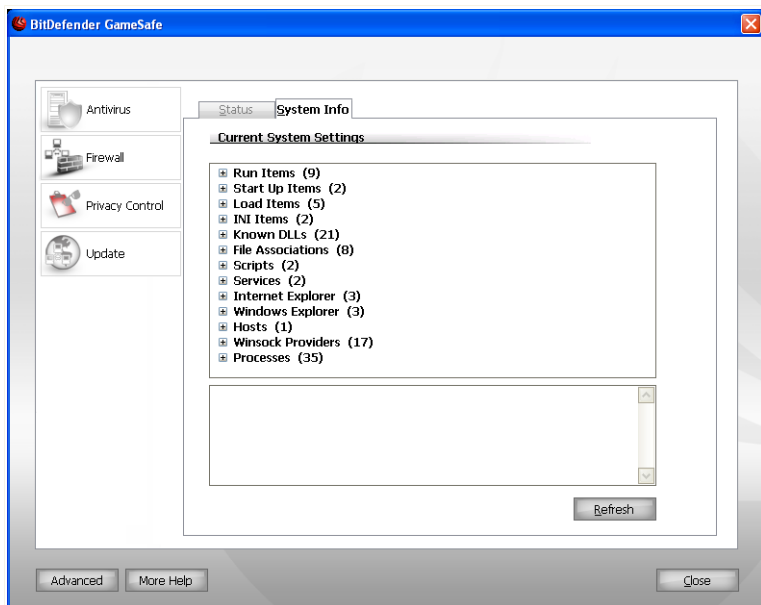
Click **Finish**.

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

10.6. 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, click **Privacy Control>System Info** in the settings console. The following window will appear:



System Information

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

Three buttons are available:

- **Remove** - deletes the selected item. You must click **Yes** to confirm your choice.



Note

If you do not want to be prompted again to confirm your choice during the current session, check **Don't ask me again this session**.

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


**Note**

Depending on the selected item, one or both of the **Remove** or **Go to** buttons may not appear.

10.7. Antiphishing Toolbar

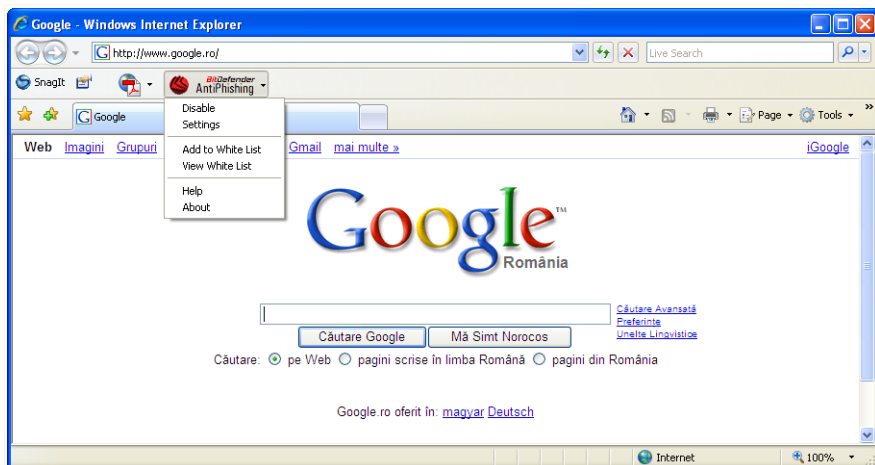
BitDefender protects you against phishing attempts when you are surfing the Internet. It scans the accessed web sites and alerts you if there are any phishing threats. A White List of web sites that will not be scanned by BitDefender can be configured.

You can easily and efficiently manage antiphishing protection and the White List using the BitDefender Antiphishing toolbar integrated into Internet Explorer.

The antiphishing toolbar, represented by the  **BitDefender icon**, is located on the topside of Internet Explorer. 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**.



Antiphishing Toolbar

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.

11. 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 was detected, depending on the options set in the **Automatic Update Settings** section, you will be asked to confirm the update or the update will be made automatically.

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:

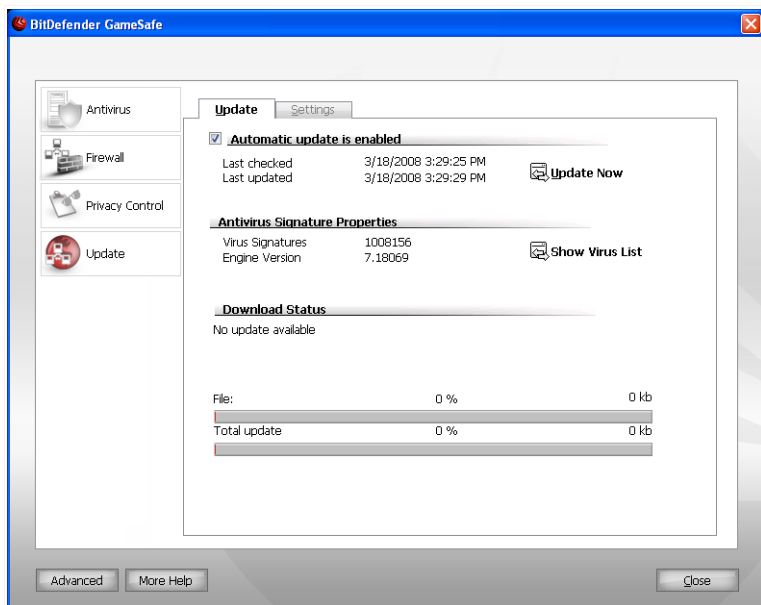
- **Updates for the antivirus engines** - as new threats appear, the files containing virus signatures must be updated to ensure permanent up-to-date protection against them. This update type is also known as **Virus Definitions Update**.
- **Updates for the antispware engines** - new spyware signatures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

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

- **Automatic Update**
- **Update Settings**


11.1. Automatic Update

To see update-related information and perform automatic updates, click **Update>Update** in the settings console. The following window will appear:



Automatic Update

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.

You can get the malware signatures of your BitDefender by clicking  **Show Virus List**. A HTML file that contains all the available signatures will be created 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.


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.

11.1.1. 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.

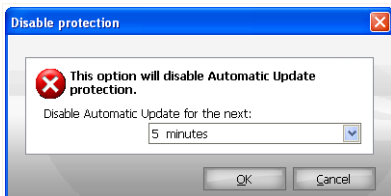


Note

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

11.1.2. Disabling Automatic Update

If you want to disable automatic update, a warning window will appear.



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.



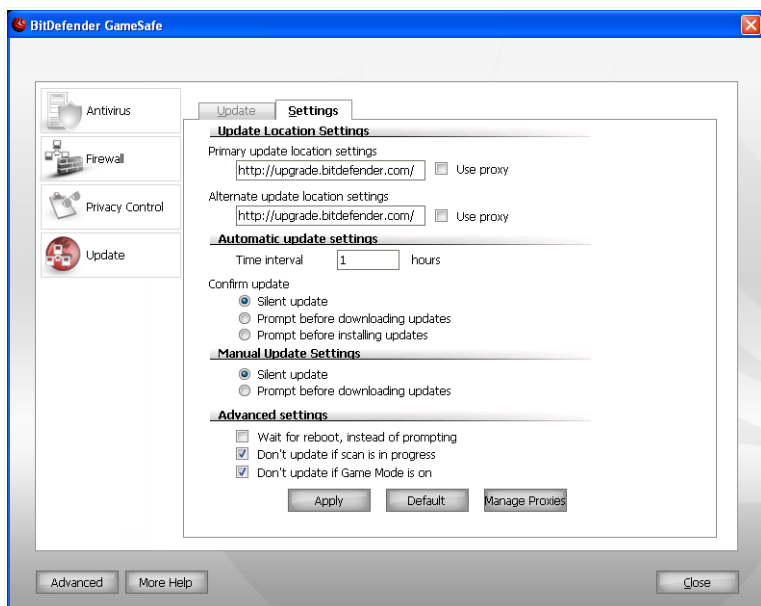
Warning

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.

11.2. 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, click **Update>Settings** in the settings console. The following window will appear:



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.

11.2.1. 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.

**Note**

For more information, please refer to *"Managing Proxies"* (p. 134)

11.2.2. 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.

**Note**

You will be prompted before updates are downloaded even if you exit the Security Center.

- **Prompt before installing updates** - every time an update was downloaded, you will be prompted before installing it.

**Note**

You will be prompted before updates are installed even if you exit the Security Center.

11.2.3. *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.

**Note**

You will be prompted before updates are downloaded even if you exit the Security Center.

11.2.4. *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.

11.2.5. 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.

Proxy Manager

Proxy Settings

Administrator proxy settings (detected at install time)

Address : Port : Username :
 Password :

Current user proxy settings (from default browser)

Address : Port : Username :
 Password :

Specify your own proxy settings

Address : Port : Username :
 Password :

OK Cancel

Proxy 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.

BitDefender Rescue CD

12. Overview

BitDefender GameSafe 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/

12.1. 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.

12.2. 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.

Top

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](#).

lpraf

lpraf is an IP Network Monitoring Software.

For more information, please refer to the [lpraf homepage](#).

lftop

lftop displays bandwidth usage on an interface.

For more information, please refer to the [lftop 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

i810rotate 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](#).

13. 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.

13.1. 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.



Boot Splash Screen

At the 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.


```

X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufsd) (aufsd) (aufsd) (aufsd)
(ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
(s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksuspend)
(aio/0) Done.
Waiting for processes to finish.....
Killing processes with signal 9: (init) (aufsd) (aufsd) (aufsd) (aufsd)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/0)
(d) (khpbspkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].

```

Wait for this message when shutting down

13.3. 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/
```

13.4. 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**.

13.5. 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.
2. Wait until BitDefender Rescue CD finishes booting. The following window will appear.



Desktop Screen

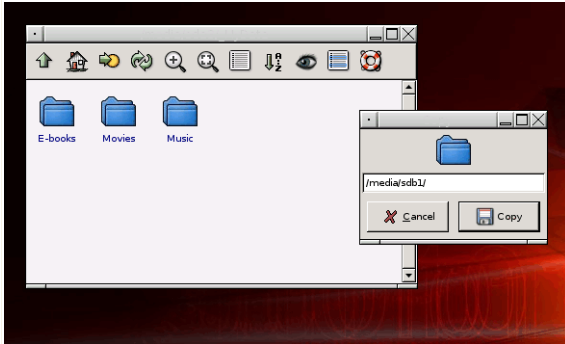
3. Double-click the partition where the data you want to save is located (e.g. [sda3]).



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.

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.



Saving Data

6. Type `/media/sdb1/` into the corresponding textbox and click **Copy**.

Getting Help

14. 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.

14.1. BitDefender Knowledge Base

The BitDefender Knowledge Base is an online repository of information about the BitDefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bugfixing activities of the BitDefender support and development teams, along with more general articles about virus prevention, the management of BitDefender solutions with detailed explanations, and many other articles.

The BitDefender Knowledge Base is open to the public and freely searchable. The extensive information it contains is yet another means of providing BitDefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from BitDefender clients eventually find their way into the BitDefender Knowledge Base, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The BitDefender Knowledge Base is available any time at <http://kb.bitdefender.com>.

14.2. Asking for Help

14.2.1. 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 link: www.bitdefender.com/gamesafe

14.3. 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.

14.3.1. Web Addresses

Sales department: sales@bitdefender.com

Technical support: support@bitdefender.com

Documentation: documentation@bitdefender.com

Partner Program: partners@bitdefender.com

Marketing: marketing@bitdefender.com

Media Relations: pr@bitdefender.com

Job Opportunities: jobs@bitdefender.com

Virus Submissions: virus_submission@bitdefender.com

Spam Submissions: spam_submission@bitdefender.com

Report Abuse: abuse@bitdefender.com

Product web site: <http://www.bitdefender.com>

Product ftp archives: <ftp://ftp.bitdefender.com/pub>

Local distributors: http://www.bitdefender.com/partner_list

BitDefender Knowledge Base: <http://kb.bitdefender.com>

14.3.2. 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

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

Technical support:

- E-mail: support@bitdefender.com
- Phone:
 - 1-888-868-1873 (Registered Users Only; accessible in United States only)
 - 1-954-776-6262 (Registered Users Only)

Customer Service:

- E-mail: customerservice@bitdefender.com
- Phone:
 - 1-888-868-1873 (Registered Users Only; accessible in United States only)
 - 1-954-776-6262 (Registered Users Only)

Germany

BitDefender GmbH

Headquarter Western Europe

Karlsdorferstrasse 56

88069 Tettnang

Germany

Tel: +49 7542 9444 60

Fax: +49 7542 9444 99

Email: info@bitdefender.com

Sales: sales@bitdefender.com

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

Technical Support: support@bitdefender.com

UK and Ireland

One Victoria Square

Birmingham

B1 1BD

Tel: +44 207 153 9959

Fax: +44 845 130 5069

Email: info@bitdefender.com
Sales: sales@bitdefender.com
Web: <http://www.bitdefender.co.uk>
Technical support: support@bitdefender.com

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2a planta, 08006
Barcelona
Soporte técnico: suporte@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
5th Fabrica de Glucoza St.
Bucharest
Technical support: support@bitdefender.com
Sales: sales@bitdefender.com
Phone: +40 21 4085600
Fax: +40 21 2330763
Product web site: <http://www.bitdefender.com>

Glossary

ActiveX

ActiveX is a model for writing programs so that other programs and the operating system can call them. ActiveX technology is used with Microsoft Internet Explorer to make interactive Web pages that look and behave like computer programs, rather than static pages. With ActiveX, users can ask or answer questions, use push buttons, and interact in other ways with the Web page. ActiveX controls are often written using Visual Basic.

Active X is notable for a complete lack of security controls; computer security experts discourage its use over the Internet.

Adware

Adware is often combined with a host application that is provided at no charge as long as the user agrees to accept the adware. Because adware applications are usually installed after the user has agreed to a licensing agreement that states the purpose of the application, no offense is committed.

However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these applications collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

Archive

A disk, tape, or directory that contains files that have been backed up.

A file that contains one or more files in a compressed format.

Backdoor

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

Boot sector

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot sector also contains a program that loads the operating system.

Boot virus

A virus that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the virus to become

active in memory. Every time you boot your system from that point on, you will have the virus active in memory.

Browser

Short for Web browser, a software application used to locate and display Web pages. The two most popular browsers are Netscape Navigator and Microsoft Internet Explorer. Both of these are graphical browsers, which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.

Command line

In a command line interface, the user types commands in the space provided directly on the screen using command language.

Cookie

Within the Internet industry, cookies are described as small files containing information about individual computers that can be analyzed and used by advertisers to track your online interests and tastes. In this realm, cookie technology is still being developed and the intention is to target ads directly to what you've said your interests are. It's a double-edge sword for many people because on one hand, it's efficient and pertinent as you only see ads about what you're interested in. On the other hand, it involves actually "tracking" and "following" where you go and what you click. Understandably so, there is a debate over privacy and many people feel offended by the notion that they are viewed as a "SKU number" (you know, the bar code on the back of packages that gets scanned at the grocery check-out line). While this viewpoint may be extreme, in some cases it is accurate.

Disk drive

It's a machine that reads data from and writes data onto a disk.

A hard disk drive reads and writes hard disks.

A floppy drive accesses floppy disks.

Disk drives can be either internal (housed within a computer) or external (housed in a separate box that connects to the computer).

Download

To copy data (usually an entire file) from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online service to one's own computer. Downloading can also refer to copying a file from a network file server to a computer on the network.

E-mail

Electronic mail. A service that sends messages on computers via local or global networks.

Events

An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

False positive

Occurs when a scanner identifies a file as infected when in fact it is not.

Filename extension

The portion of a filename, following the final point, which indicates the kind of data stored in the file.

Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

Heuristic

A rule-based method of identifying new viruses. This method of scanning does not rely on specific virus signatures. The advantage of the heuristic scan is that it is not fooled by a new variant of an existing virus. However, it might occasionally report suspicious code in normal programs, generating the so-called "false positive".

IP

Internet Protocol - A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

Java applet

A Java program which is designed to run only on a web page. To use an applet on a web page, you would specify the name of the applet and the size (length and width, in pixels) that the applet can utilize. When the web page is accessed, the browser downloads the applet from a server and runs it on the user's machine (the client). Applets differ from applications in that they are governed by a strict security protocol.

For example, even though applets run on the client, they cannot read or write data onto the client's machine. Additionally, applets are further restricted so that they can only read and write data from the same domain that they are served from.

Macro virus

A type of computer virus that is encoded as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support powerful macro languages.

These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened.

Mail client

An e-mail client is an application that enables you to send and receive e-mail.

Memory

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips, and the word storage is used for memory that exists on tapes or disks. Every computer comes with a certain amount of physical memory, usually referred to as main memory or RAM.

Non-heuristic

This method of scanning relies on specific virus signatures. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a virus, and does not generate false alarms.

Packed programs

A file in a compression format. Many operating systems and applications contain commands that enable you to pack a file so that it takes up less memory. For example, suppose you have a text file containing ten consecutive space characters. Normally, this would require ten bytes of storage.

However, a program that packs files would replace the space characters by a special space-series character followed by the number of spaces being replaced. In this case, the ten spaces would require only two bytes. This is just one packing technique - there are many more.

Path

The exact directions to a file on a computer. These directions are usually described by means of the hierarchical filing system from the top down.

The route between any two points, such as the communications channel between two computers.

Phishing

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as

passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Polymorphic virus

A virus that changes its form with each file it infects. Since they have no consistent binary pattern, such viruses are hard to identify.

Port

An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Report file

A file that lists actions that have occurred. BitDefender maintains a report file listing the path scanned, the folders, the number of archives and files scanned, how many infected and suspicious files were found.

Rootkit

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

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

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

Script

Another term for macro or batch file, a script is a list of commands that can be executed without user interaction.

Spam

Electronic junk mail or junk newsgroup postings. Generally known as any unsolicited e-mail.

Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Startup items

Any files placed in this folder will open when the computer starts. For example, a startup screen, a sound file to be played when the computer first starts, a reminder calendar, or application programs can be startup items. Normally, an alias of a file is placed in this folder rather than the file itself.

System tray

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right click an icon to view and access the details and controls.

TCP/IP

Transmission Control Protocol/Internet Protocol - A set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

Trojan

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

BitDefender has its own update module that allows you to manually check for updates, or let it automatically update the product.

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Virus definition

The binary pattern of a virus, used by the antivirus program to detect and eliminate the virus.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.