bitdefender

ANTIVIRUS 2008

User's guide

BitDefender Antivirus 2008

User's guide

Published 2007.11.29

Legal Notice


bitdefender

Table of Contents

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 Antivirus 2008** as a security solution for their personal computers. The information presented in this book is suitable not only for computer literates, it is accessible to everyone who is able to work under Windows.

This book will describe for you **BitDefender Antivirus 2008**, the Company and the team who built it, will guide you through the installation process, will teach you how to configure it. You will find out how to use **BitDefender Antivirus 2008**, how to update, test and customize it. You will learn how to get best from BitDefender.

We wish you a pleasant and useful lecture.

1. Conventions Used in This Book

1.1. Typographical Conventions

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

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

1.2. Admonitions

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

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

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

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

2. The Book Structure

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

Installation. Step by step instructions for installing BitDefender on a workstation. This is a comprehensive tutorial on installing **BitDefender Antivirus 2008**. Starting with the prerequisites for a successfully installation, you are guided through the whole installation process. Finally, the removing procedure is described in case you need to uninstall BitDefender.

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

Advanced 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 Antivirus 2008 Installation

The **BitDefender Antivirus 2008 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 Antivirus 2008 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 Antivirus 2008:

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

2. Click **Next**.

   BitDefender Antivirus 2008 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 Antivirus 2008 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 Antivirus 2008 to be installed.

   Click **Next**.
5. Select options regarding the installation process. Some of them will be selected by default:
   - **Open readme file** - to open the readme file at the end of the installation.
   - **Place a shortcut on the desktop** - to place a shortcut to BitDefender Antivirus 2008 on your desktop at the end of the installation.
   - **Eject CD when installation is complete** - to have the CD ejected at the end of the installation; this option appears when you install the product from the CD.
   - **Turn off Windows Defender** - to turn off Windows Defender; this option appears only on Windows Vista.

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

   Important
   During the installation process a wizard will appear. The wizard helps you register your **BitDefender Antivirus 2008**, 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.

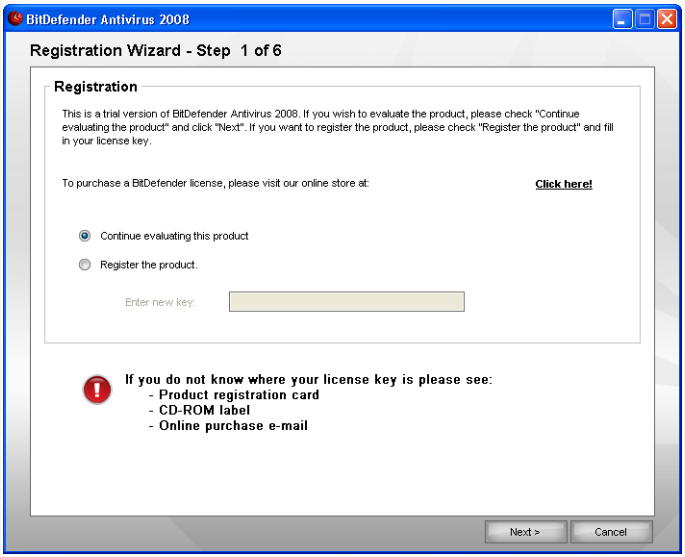
   If you have accepted the default settings for the installation path, you can see in `Program Files` a new folder, named `BitDefender`, which contains the subfolder `BitDefender 2008`.

1.3. Initial Setup Wizard

During the installation process a wizard will appear. The wizard helps you register your **BitDefender Antivirus 2008**, create a BitDefender account and set BitDefender to perform important security tasks.

Completing this wizard is not mandatory; however, we recommend you do so in order to save time and ensure your system is safe even before BitDefender Antivirus 2008 is installed.

1.3.1. Step 1/6 - Register BitDefender Antivirus 2008



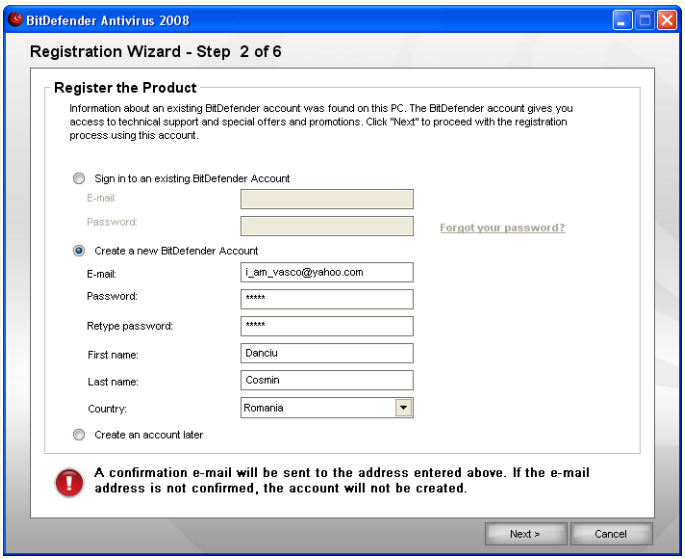
Registration

Choose **Register the product** to register **BitDefender Antivirus 2008**. 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. Select **Create a new BitDefender account** and provide the required information. The data you provide here will remain confidential.

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

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

Note
The password must be least four characters long.

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

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 or **Cancel** to exit the wizard.

I already have a BitDefender account

If you already have an active account, select **Sign in to an existing BitDefender Account** and provide the e-mail address and the password of your account.

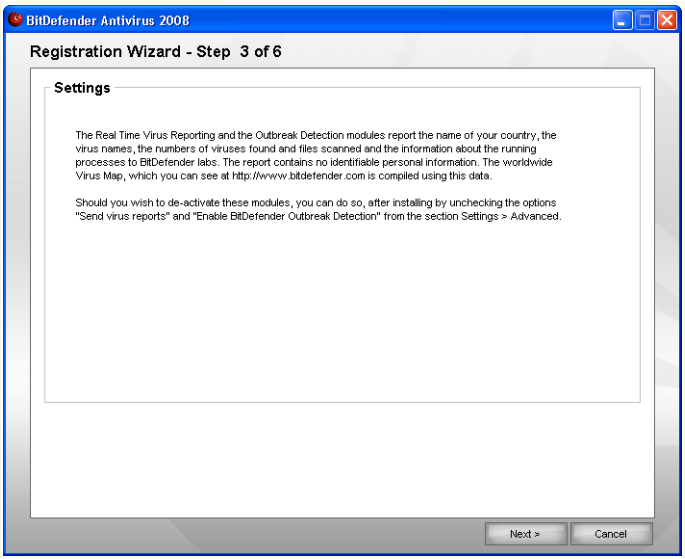
Note

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 or **Cancel** to exit the wizard.

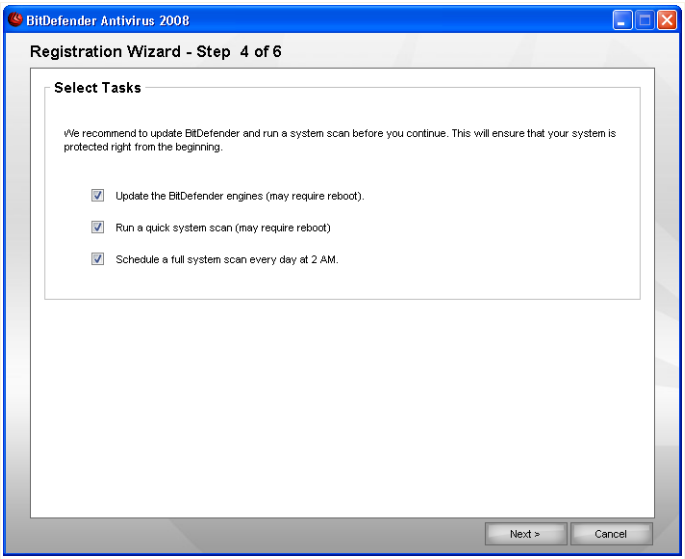
1.3.3. Step 3/6 - Learn about Real-Time Virus Reporting (RTVR)



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 Antivirus 2008 to perform important tasks for the security of your system.

The following options are available:

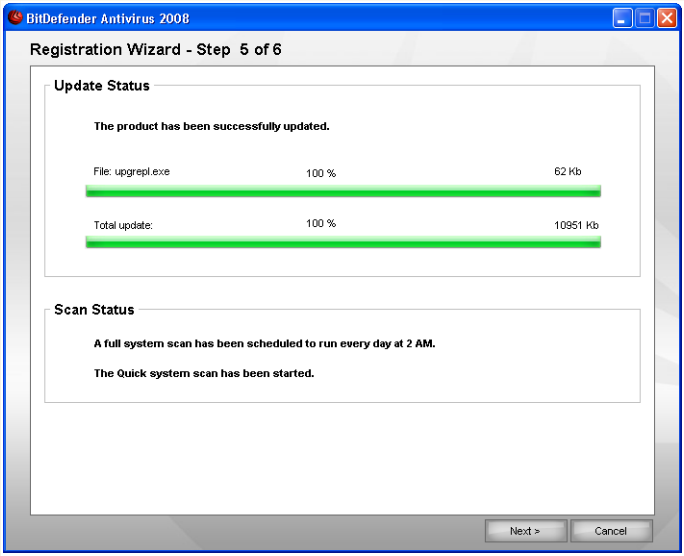
- **Update the BitDefender engines (may require reboot)** - during the next step, an update of the BitDefender engines will be performed in order to protect your computer against the latest threats.
- **Run a quick system scan (may require reboot)** - during the next step, a quick system scan will be 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

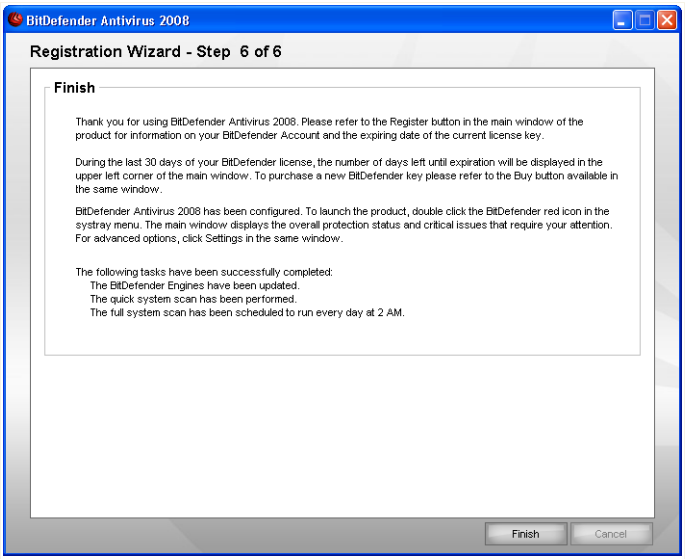


Task Status

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

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

1.3.6. Step 6/6 - View Summary



Finish

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 one of the following ways:

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

  Double-click the setup file and follow the wizard described in the "*Installation Steps*" (p. 3) section.

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

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

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

Important
If you upgrade from BitDefender v8 or higher, we recommend you save the BitDefender settings, the Friends list and the Spammers list. After the upgrade process is over, you may load them.

1.5. Repairing or Removing BitDefender

If you want to repair or remove **BitDefender Antivirus 2008**, 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.

Important
Before repairing the product we recommend you save the Friends list and the Spammers list. You can also save the BitDefender settings and the Bayesian database. After the repair process is over you may reload them.

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

Restart the computer when prompted and, afterwards, click **Install** to reinstall BitDefender Antivirus 2008.

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 malware threats, such as viruses and spyware. If you want Windows Defender to be enabled after

uninstalling BitDefender, select the corresponding check box. This option is available only on Windows Vista.

Click **Remove** to start the removal of BitDefender Antivirus 2008 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 Antivirus 2008** 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.

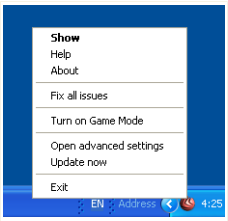
- The **Quick Tasks** area: helps you keep your system safe and protect your data.

Furthermore, the BitDefender Security Center contains several useful shortcuts.

Link	*Description*
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.



Contextual Menu

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.

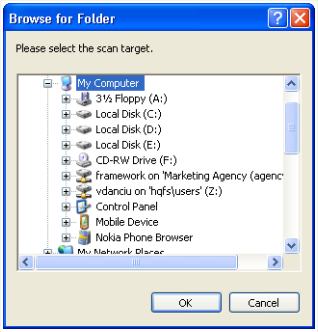
- **Show** - opens the BitDefender Security Center.
- **Help** - opens the help file.

- **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.

2.2. 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.

2.3. 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**.

2.3.1. 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.

2.3.2. 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 Antivirus 2008 will let you know whenever a problem can affect your computer's security.

There are four security status buttons:

- **ANTIVIRUS**
- **ANTIPHISING**
- **IDENTITY CONTROL**
- **UPDATE**

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.

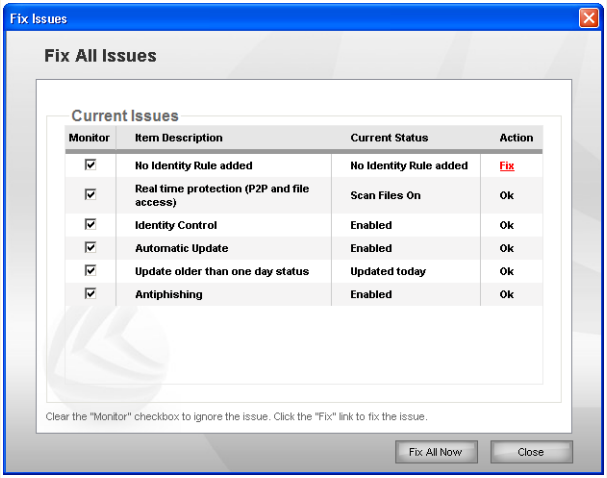
The four status buttons can be displayed in green, yellow, red or grey, depending on the current level of protection.

- **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.

You will see a list of securities 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.



Security Issues

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

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.

3.1. Antivirus Status Button

If the antivirus 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.

Issue	Color
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

To fix the issues, follow these steps:

1. Click the antivirus 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. Antiphising Status Button

If the antiphising 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.

Issue	Color
The antiphising protection is enabled	Green
The antiphising protection is disabled	Red

To fix the issues, follow these steps:

1. Click the antiphising 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.

Issue	Color
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 Identity Control 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.

3.4. Update Status Button

If the update 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.

Issue	Color
Automatic update is enabled	Green
Automatic update is disabled	Red
The last update is one day old	Red

To fix the issues, follow these steps:

1. Click the update 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 four 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.

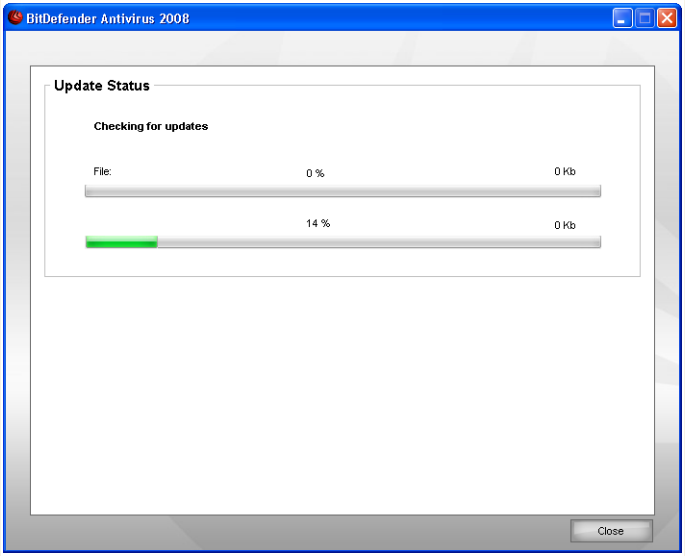
The following buttons are available:

- **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 Computer. 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: `My Documents`, `Desktop` and `StartUp`. 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.

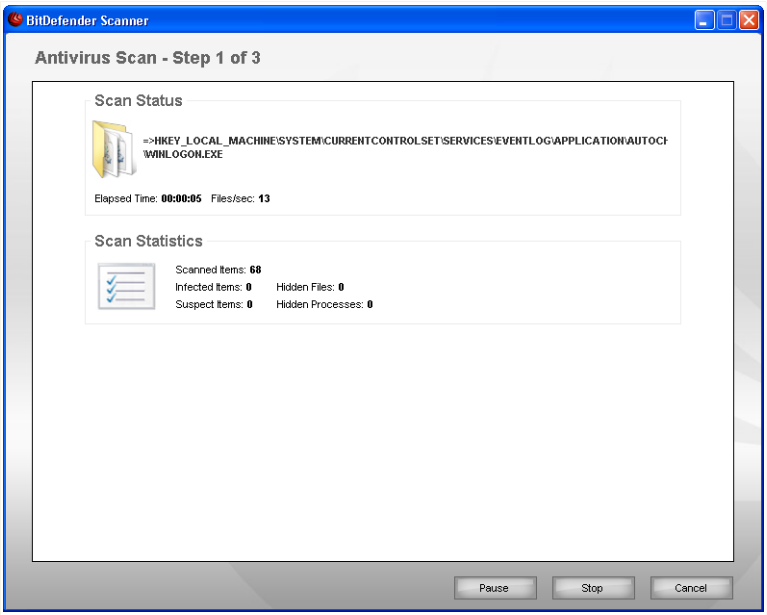
Note
Since the **Deep System Scan** and **Full System Scan** tasks analyze the entire system, the scanning may take a while. Therefore, we recommend you to run these tasks on low priority or, better, when your system is idle.

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.

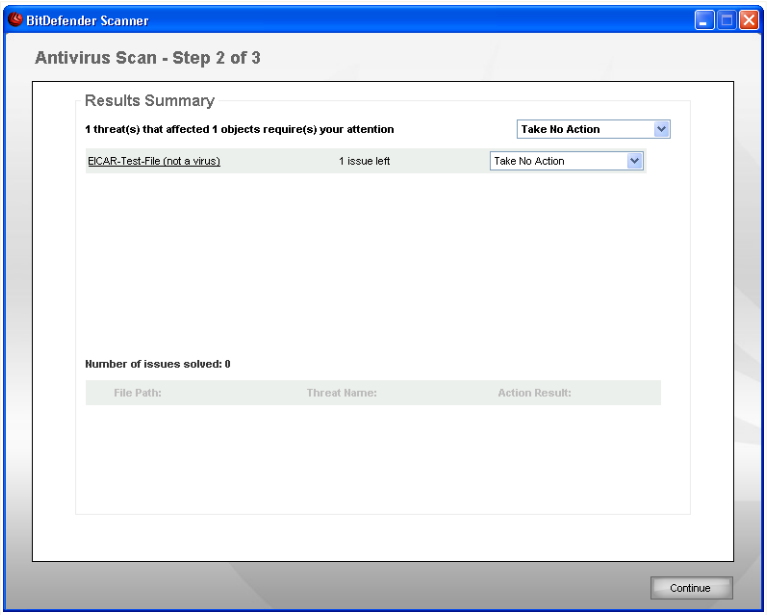
To temporarily stop the scanning process, just click **Pause**. You will have to click **Resume** to resume scanning.

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:

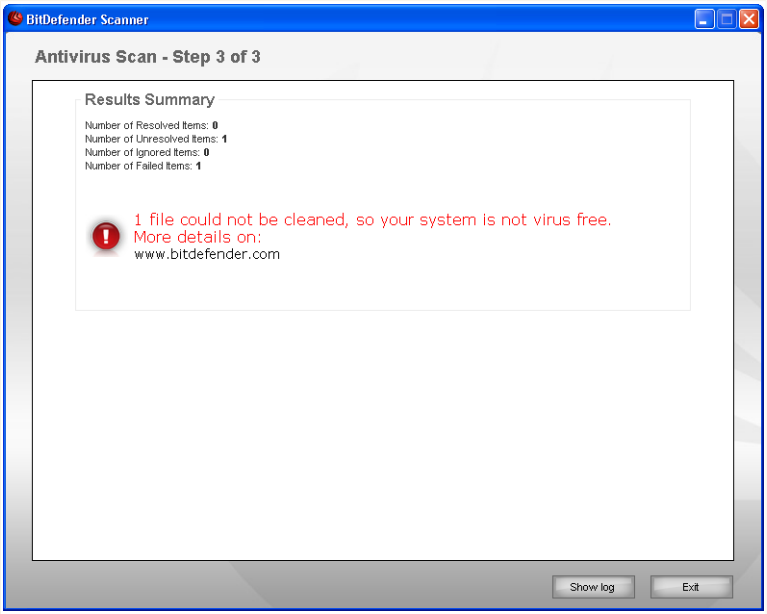
Action	Description
Take No Action	No action will be taken on the detected files.

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.

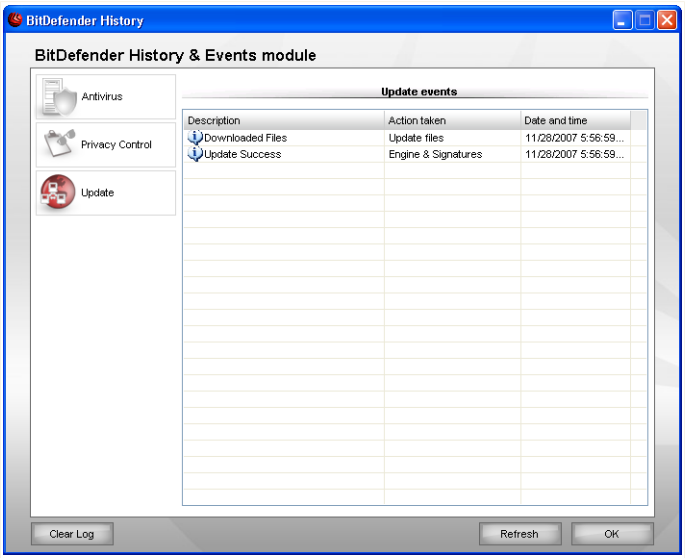
If suspect files were detected during the scan, you will be requested to submit them to the BitDefender Lab. Suspect files are files detected by the heuristic analysis and they might be infected with malware the signature of which has not been released yet.

The report file is automatically saved in the Logs section from the **Properties** window of the respective task.

Warning
If there are unsolved issues, we recommend you to contact the BitDefender Support Team at www.bitdefender.com.

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, if your backup tasks run without error, etc.



Events

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

- **Antivirus**
- **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.

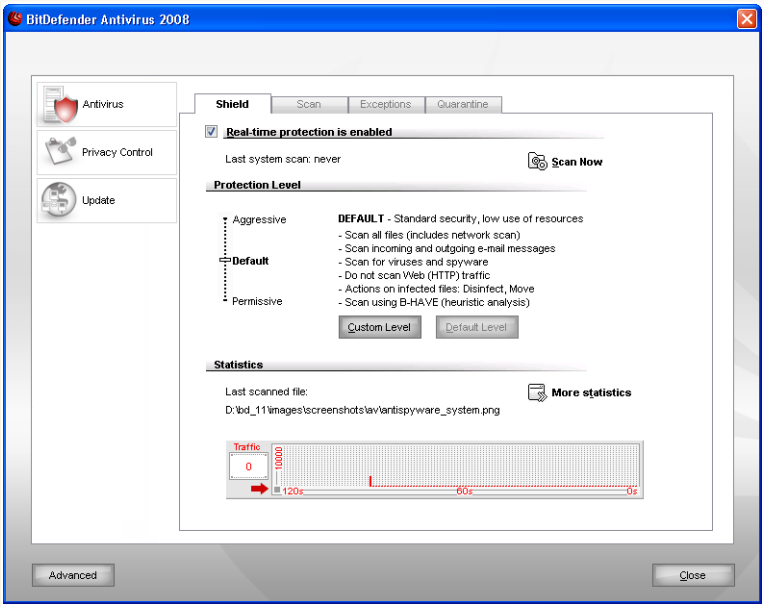
Click **Clear Log** if you want to remove old logs or **Refresh** to make sure the latest logs are displayed.

Advanced Security Administration

6. Getting Started

BitDefender Antivirus 2008 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

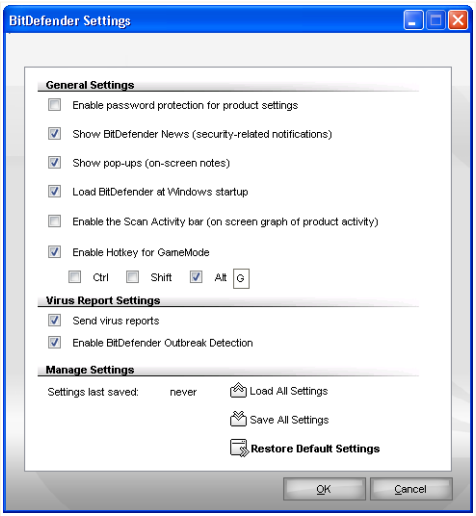
The settings console is organized into modules: **Antivirus**, **Privacy Control** and **Update**. This allows you to easily manage BitDefender based on the type of security issue addressed.

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

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

6.1. Configuring General Settings

To configure general settings for BitDefender Antivirus 2008 and to manage its settings, click **Advanced**. A new window will appear.



General Settings

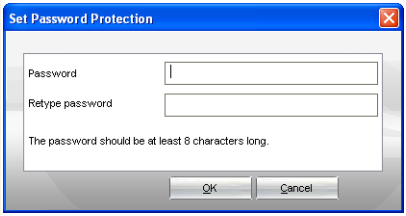
Here you can set the overall behavior of BitDefender. By default, BitDefender is loaded at Windows startup and then runs minimized in the taskbar.

6.1.1. 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)** - enables/disables the Scan Activity Bar.
- **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.

6.1.2. 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.

6.1.3. 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.

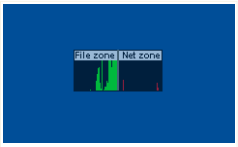
Important
Only users with administrative rights can save and load settings.

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

6.2. Using 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.



Activity Bar

Note
The Scan activity bar will notify you when real-time protection is disabled by displaying a red cross over the **File Zone**.

You can use the **Scan activity bar** to scan objects. Just drag the objects that you want to be scanned and drop them over it.

Note
For more information, please refer to "*Drag&Drop Scanning*" (p. 59).

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)**.

7. 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:

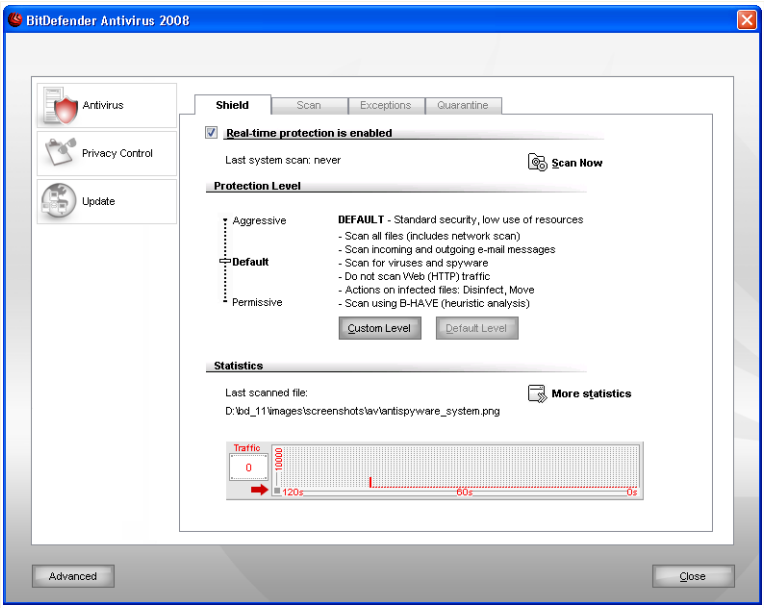
- **On-access scanning** - prevents new malware threats from entering your system. This is also called real-time protection - files are scanned as you use them - on-access. BitDefender will, for example, scan a word document for known threats when you open it, and an e-mail message when you receive one.
- **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:

7.1. 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**.

7.1.1. 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:

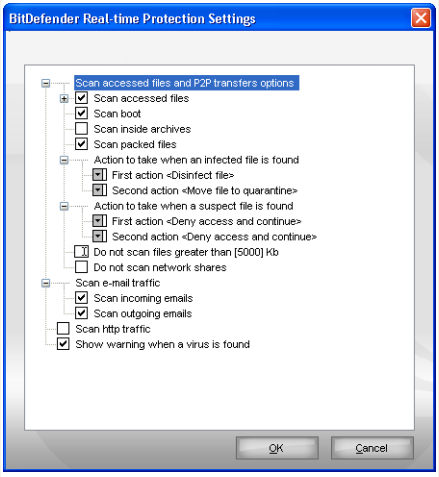
Protection level	Description
Permissive	Covers basic security needs. The resource consumption level is very low. Programs and incoming mail messages are only scanned for viruses. Besides the classical signature-based scan, the heuristic analysis is also used. The actions taken on infected files are the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

7.1.2. 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
		.scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml and .nws.
	Scan user defined extensions	Only the files with the extensions specified by the user will be scanned. These extensions must be separated by ";".
	Scan for riskware	Scans for riskware. Detected files will be treated as infected. The software that includes adware components might stop working if this option is enabled. Select **Skip dialers and applications from scan** if you want to exclude these kind of files from scanning.
Scan boot		Scans the system's boot sector.
Scan inside archives		The accessed archives will be scanned. With this option on, the computer will slow down.
Scan packed files		All packed files will be scanned.
First action		Select from the drop-down menu the first action to take on infected and suspicious files.
	Deny access and continue	In case an infected file is detected, the access to this will be denied.
	Clean file	Disinfects infected files.
	Delete file	Deletes infected files immediately, without any warning.
	Move file to quarantine	Moves infected files into the quarantine.

Option		Description
Second action		Select from the drop-down menu the second action to take on infected files, in case the first action fails.
	Deny access 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:

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

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

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

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

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

7.1.3. 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.

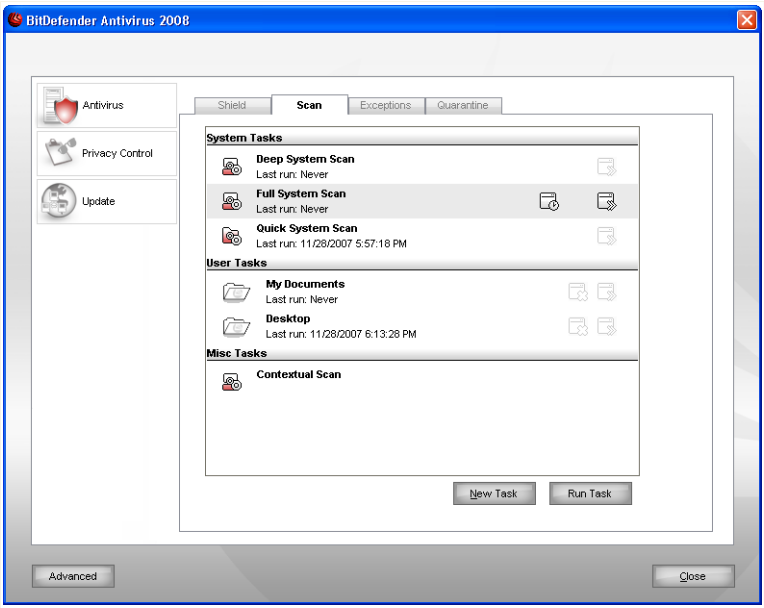
Warning
This is a critical security issue. We recommend you to disable real-time protection for as little time as possible. If real-time protection is disabled, you will not be protected against malware threats.

7.2. 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

7.2.1. 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. 47).

There are three categories of scan tasks:

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

Default Task	Description
Deep System Scan	Scans the entire system. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.
Full System Scan	Scans the entire system, except for archives. In the default configuration, it scans for all types of malware threatening your system's security, such as viruses, spyware, adware, rootkits and others.
Quick System Scan	Scans the `Windows`, `Program Files` and `All Users` folders. In the default configuration, it scans for all types of malware, except for rootkits, but it does not scan memory, the registry or cookies.

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.

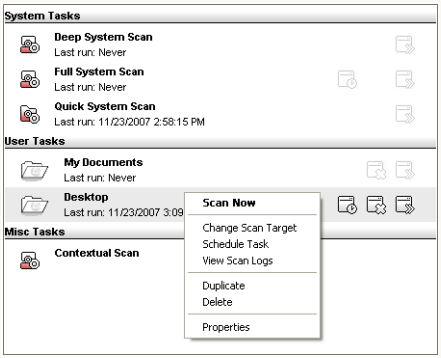
To the left of each task you can see the **Properties** button, that allows you to configure the task and view the scan logs.

7.2.2. 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.



Shortcut Menu

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

- **Schedule 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.

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.

7.2.3. 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.

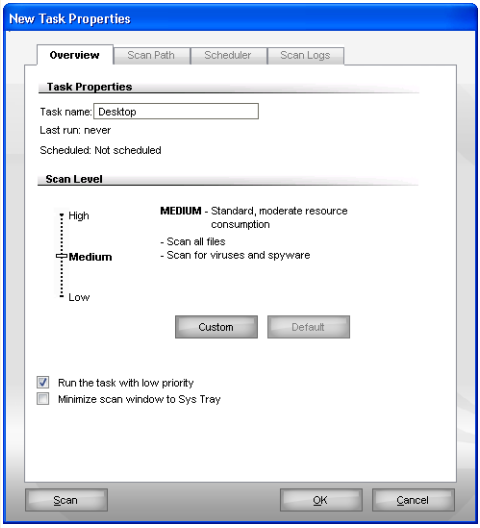
7.2.4. Configuring Scan Tasks

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. 64).

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.

Protection level	Description
	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:

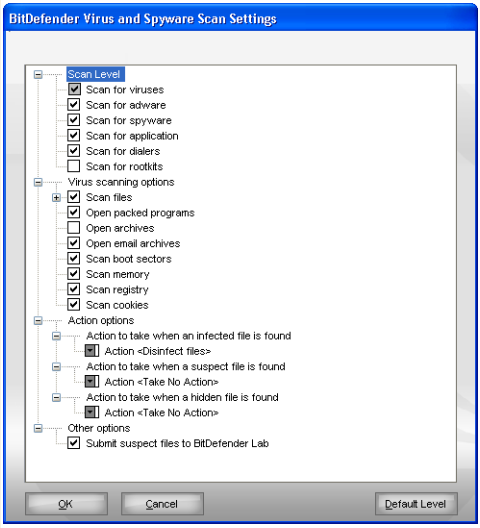
Option	Description
Run the task with Low priority	Decreases the priority of the scan process. You will allow other programs to run faster and increase the time needed for the scan process to finish.
Minimize scan window on start to systray	Minimizes the scan window to the system tray. Double-click the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

Option	Description
Scan for viruses	Scans for known viruses.

Option	Description
	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:

Option		Description
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`.

Option		Description
	Scan user defined extensions	Only the files with the extensions specified by the user will be scanned. These extensions must be separated by ";".
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:

Action	Description
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:

Action	Description
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.

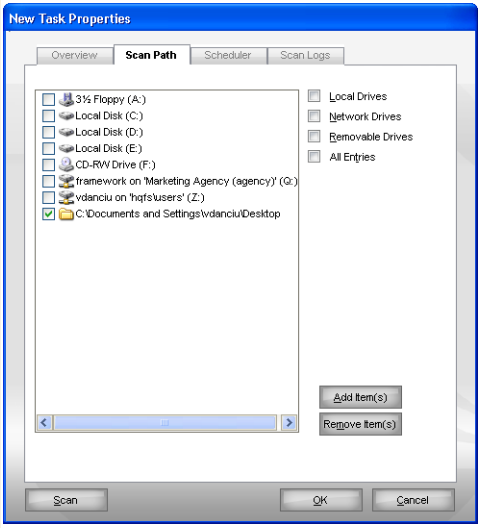
Note
If you choose to ignore the detected files or if the chosen action fails, you will have to choose an action in the scanning wizard.

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

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

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

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

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

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

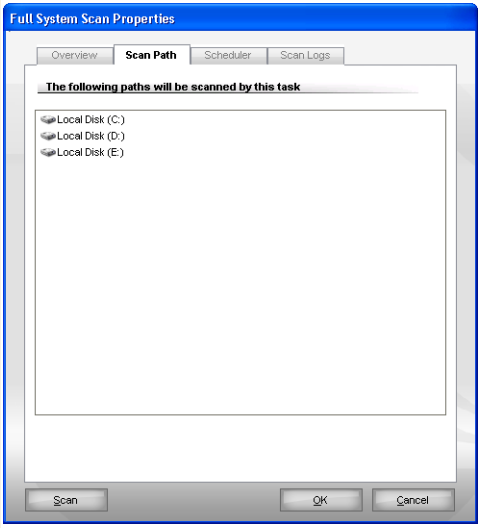
Note
If you want to scan your entire computer, select the checkbox corresponding to **All Entries**.

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

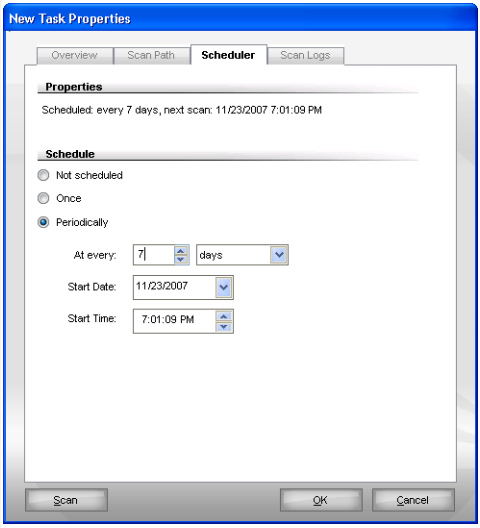
Full System Scan and **Deep System Scan** will scan all local drives, while **Quick System Scan** will only scan the `Windows` and `Program Files` folders.

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**.

7.2.5. 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.

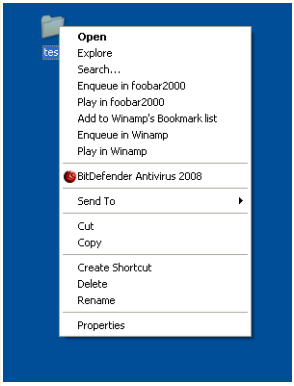
To run a scan task, use one of the following methods:

- 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. 60).

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

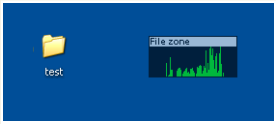
Right-click the file or folder you want to be scanned and select **BitDefender Antivirus 2008**.

The BitDefender Scanner will appear and the scanning will be initiated. For more information, please refer to "*BitDefender Scanner*" (p. 60).

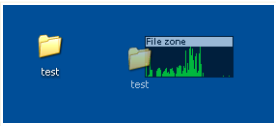
You can modify the scan options and see the report files by accessing the **Properties** window of the **Contextual Menu Scan** task.

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. 60).

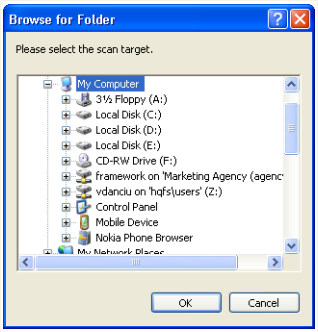
Manual Scanning

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**.

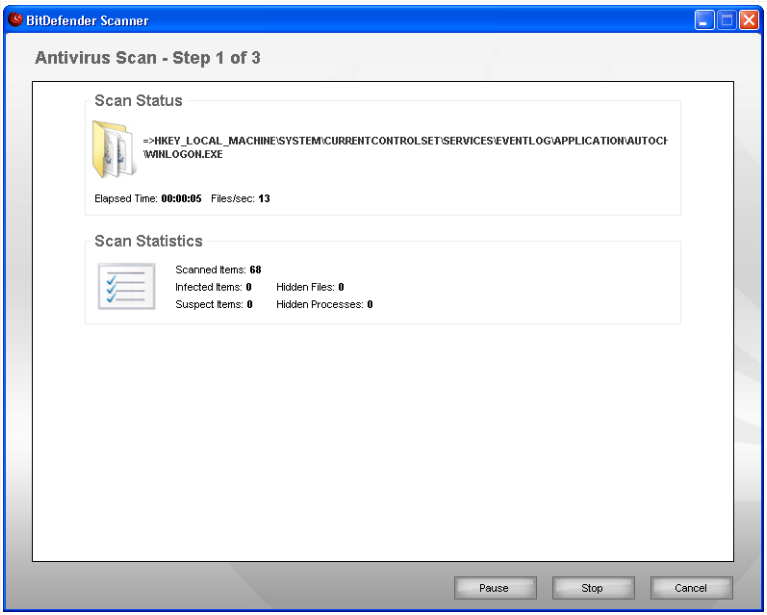
The BitDefender Scanner will appear and the scanning will be initiated. For more information, please refer to "*BitDefender Scanner*" (p. 60).

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.

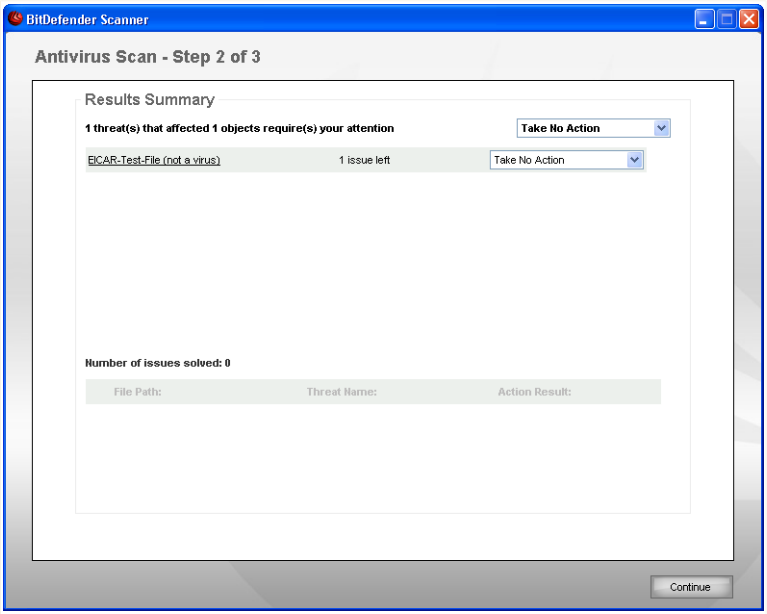
To temporarily stop the scanning process, just click **Pause**. You will have to click **Resume** to resume scanning.

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:

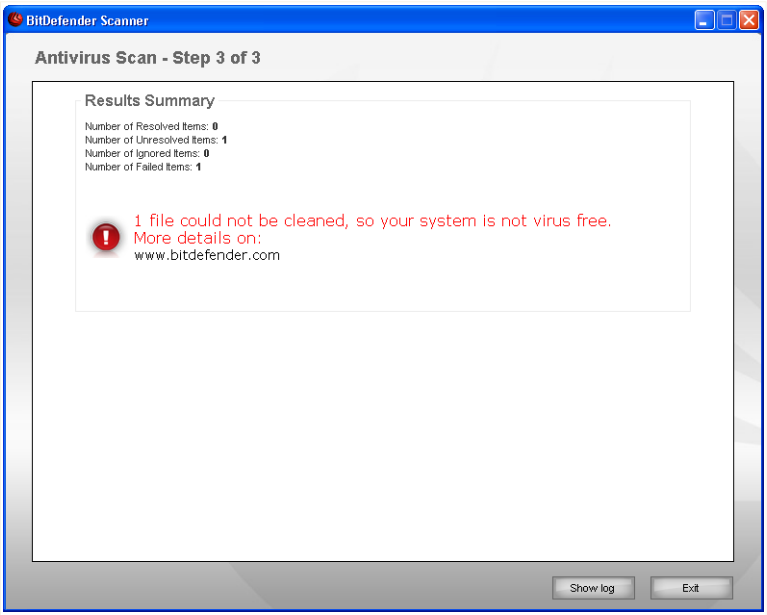
Action	Description
Take No Action	No action will be taken on the detected files.

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.

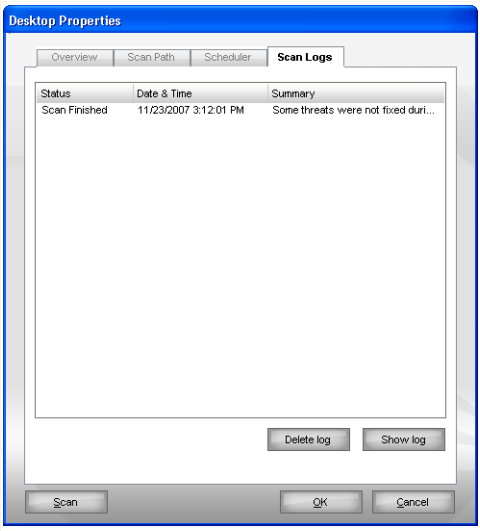
If suspect files were detected during the scan, you will be requested to submit them to the BitDefender Lab. Suspect files are files detected by the heuristic analysis and they might be infected with malware the signature of which has not been released yet.

The report file is automatically saved in the Logs section from the **Properties** window of the respective task.

Warning
If there are unsolved issues, we recommend you to contact the BitDefender Support Team at www.bitdefender.com.

7.2.6. 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:

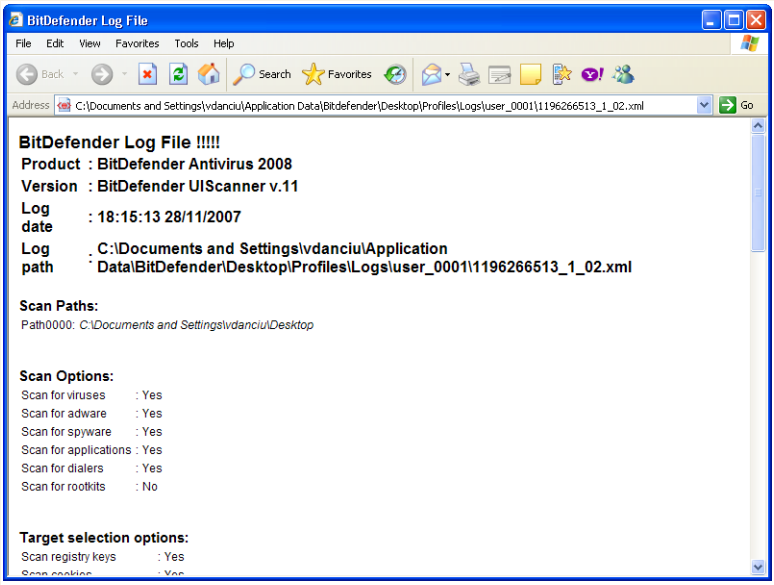
- **Delete log** - to delete the selected scan log.
- **Show log** - to view the selected scan log. The scan log will open in your default web browser.

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.

7.3. Objects Excluded from Scanning

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

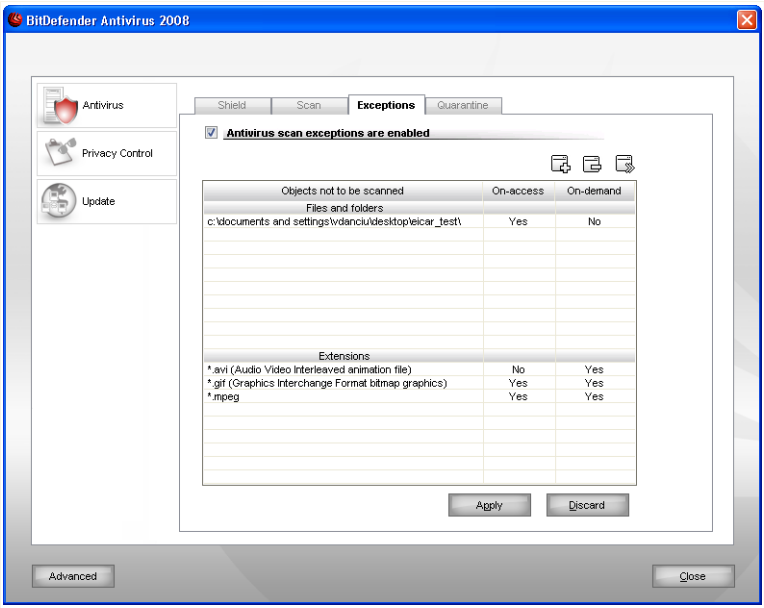
BitDefender allows excluding objects from on-access or on-demand scanning, or from both. This feature is intended to decrease scanning times and to avoid interference with your work.

Two types of objects can be excluded from scanning:

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

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

To see and manage the objects excluded from scanning, click **Antivirus>Exceptions** in the settings console. The following window will appear:



Exceptions

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

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**.

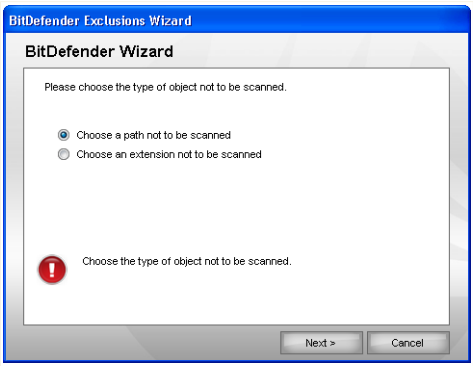
Note
You can also right-click an object and use the options on the shortcut menu to edit or delete it.

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

7.3.1. 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

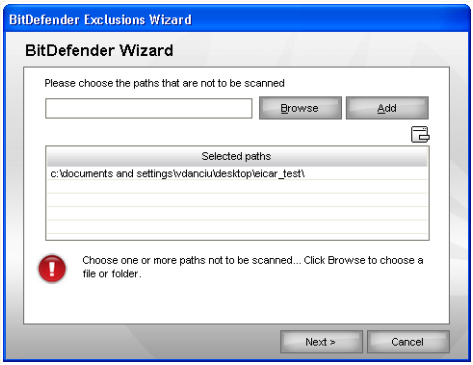


Object Type

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**.

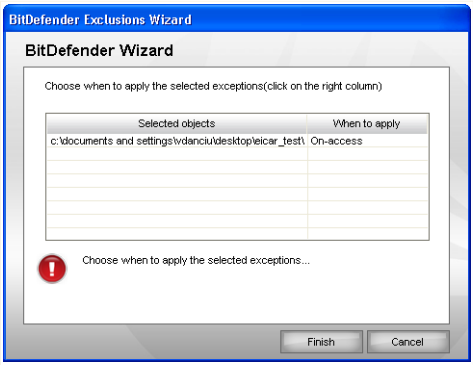
Note
If the provided path does not exist, an error message will appear. Click **OK** and check the path for validity.

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.

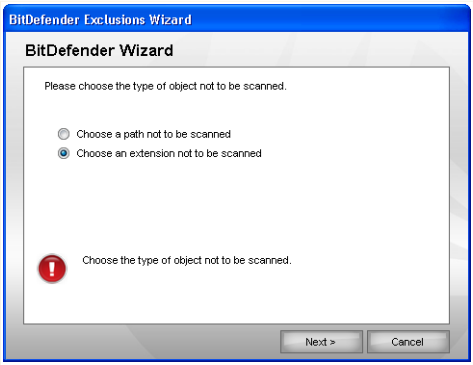
Click **Finish**.

Click **Apply** to save the changes.

7.3.2. 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

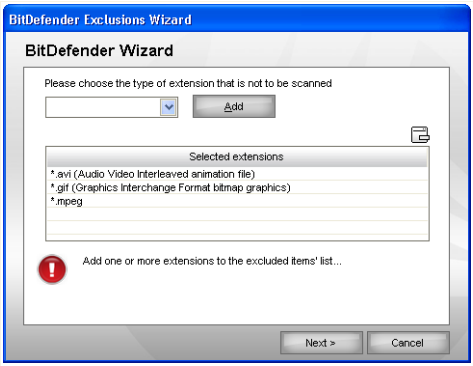


Object Type

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.

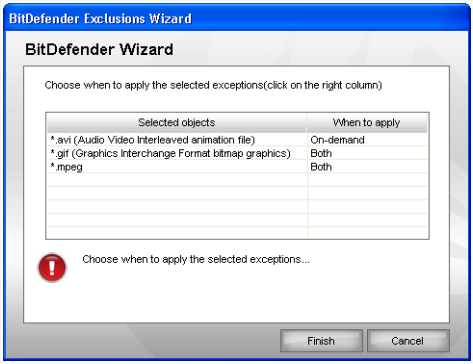
- Type the extension that you want to be excluded from scanning in the edit field and click **Add**.

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.

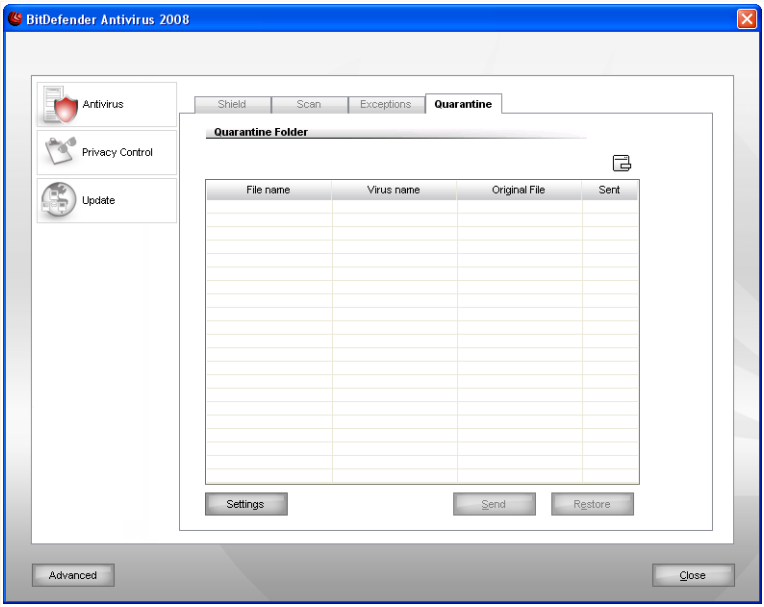
Click **Finish**.

Click **Apply** to save the changes.

7.4. 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

7.4.1. 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.

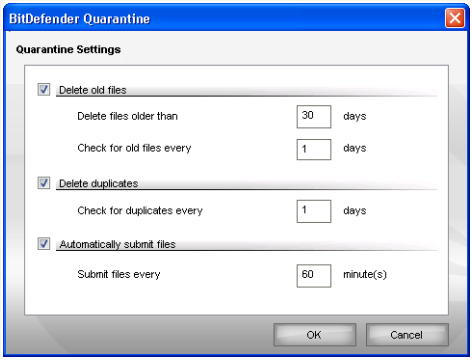
To delete a selected file from quarantine, click the **Remove** button. If you want to restore a selected file to its original location, click **Restore**.

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.

7.4.2. 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.

8. 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.

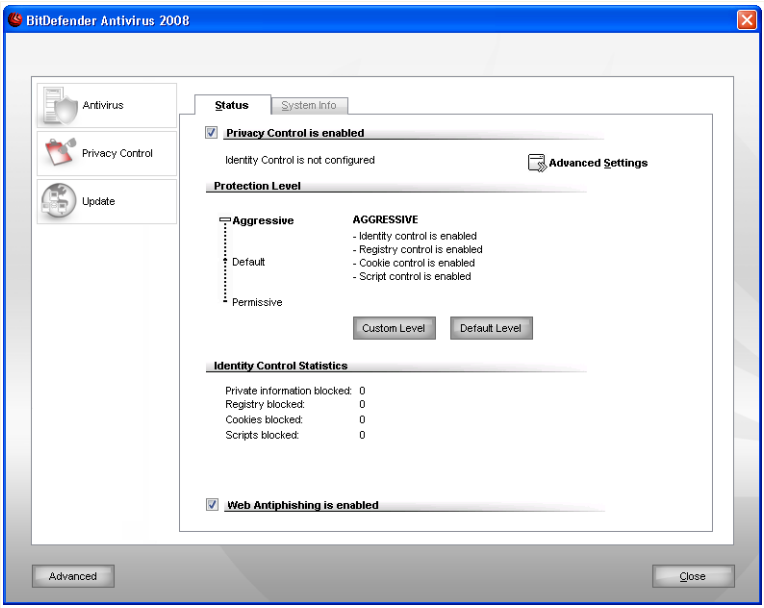
BitDefender also scans the web sites you visit and alerts you if any phishing threat is detected.

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

8.1. 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

8.1.1. 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:

Protection level	Description
Permissive	Only **Registry control** is enabled.
Default	**Registry control** and **Identity Control** are enabled.
Aggressive	**Registry control**, **Identity Control** and **Script Control** are enabled.

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

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

8.1.2. 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. 95).

8.2. 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.

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

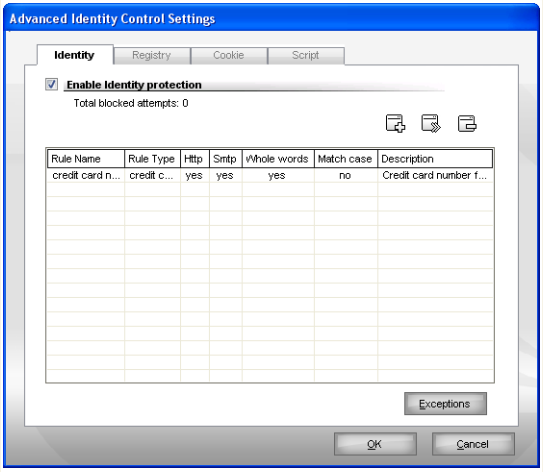
Identity Control helps you keep confidential data safe. It scans the HTTP or SMTP traffic, or both, for certain strings that you have defined. If a match is found, the respective web page or e-mail is blocked.

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**.



Identity Control

8.2.1. Creating Identity Rules

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

The configuration wizard comprises a 3 step procedure.

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

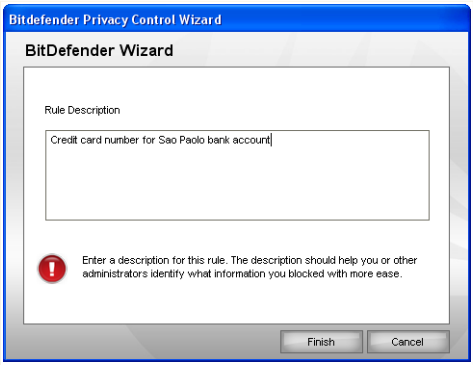
Select the type of traffic you want BitDefender to scan. The following options are available:

- **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

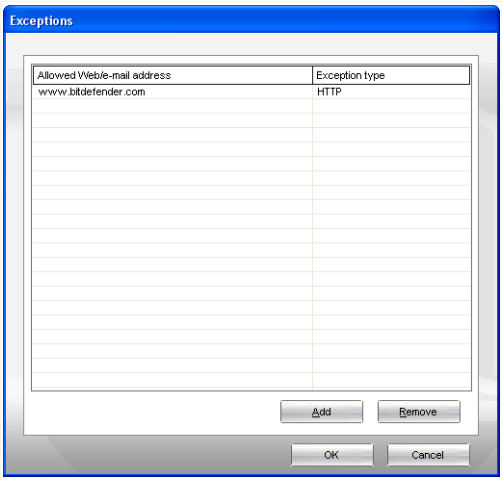
Enter a short description of the rule in the edit field.

Click **Finish**.

8.2.2. 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**.



Exceptions

To add an exception, follow these steps:

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

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

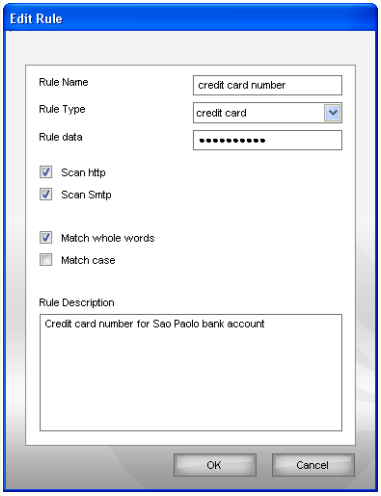
Click **OK** to save the changes.

8.2.3. Managing Rules

You can see the rules listed in the table.

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

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



Edit Rule

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

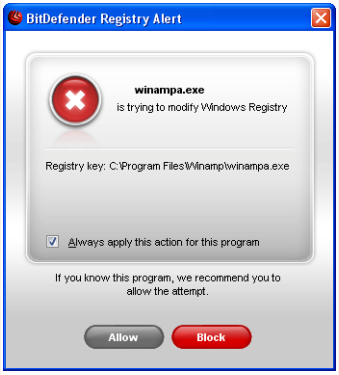
Click **OK** to save the changes and close the window.

8.3. Advanced Settings - Registry Control

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.

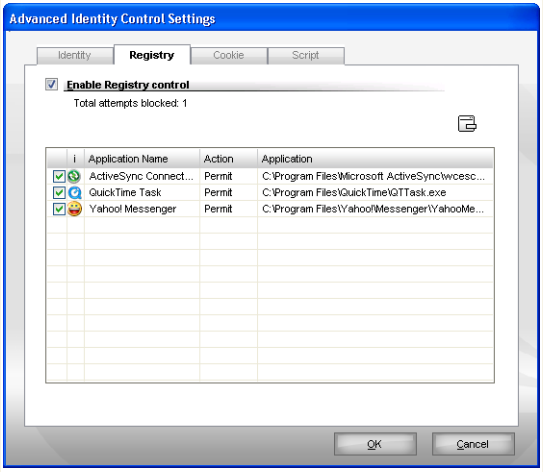
Note

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.

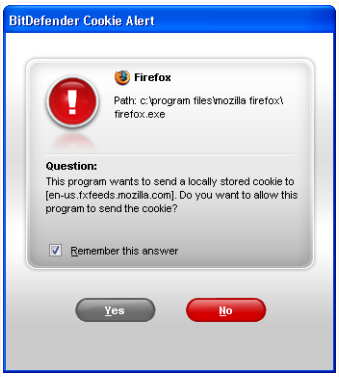
8.4. Advanced Settings - Cookie Control

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.

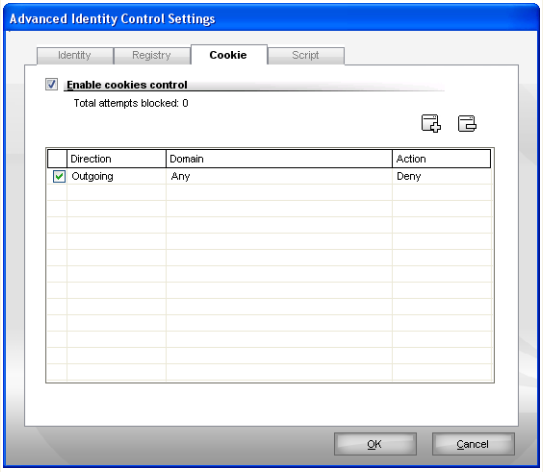
Note

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**.



Cookie Control

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

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

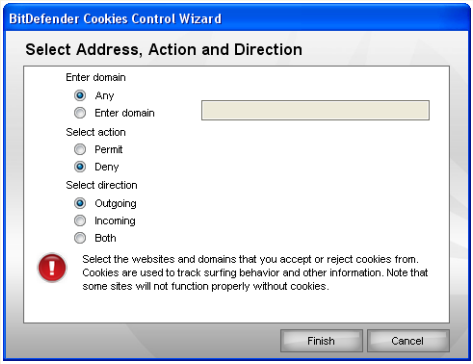
To delete a rule, just select it and click the **Delete** button. To modify a parametre of a rule just double click its field and make the desired modification. To temporarily deactivate a rule without deleting it, clear the corresponding checkbox.

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

8.4.1. Configuration Wizard

The configuration wizard is a 1 step procedure.

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.

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

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

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

Click **Finish**.

Note

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

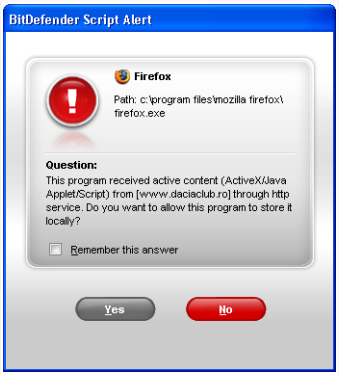
Click **OK** to save the changes and close the window.

8.5. 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:



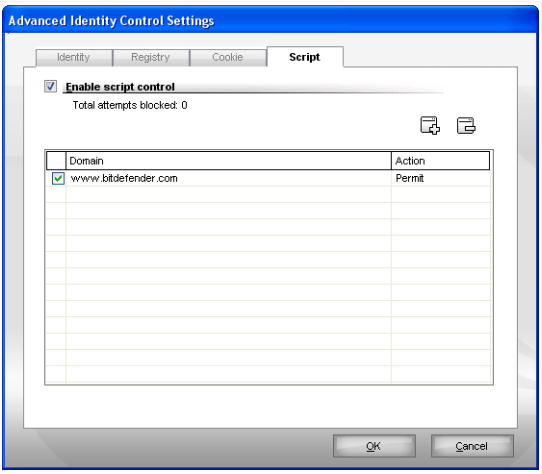
Script Alert

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.

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



Script Control

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

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

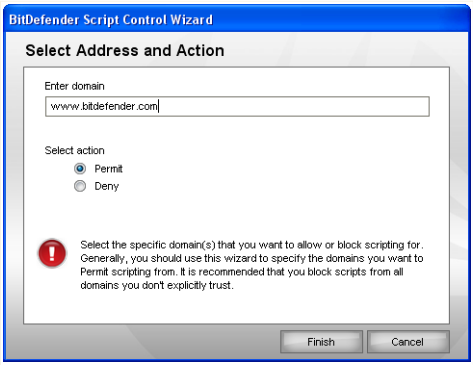
To delete a rule, just select it and click the **Delete** button. To modify a parametre of a rule just double click its field and make the desired modification. To temporarily deactivate a rule without deleting it, clear the corresponding checkbox.

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

8.5.1. Configuration Wizard

The configuration wizard is a 1 step procedure.

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.

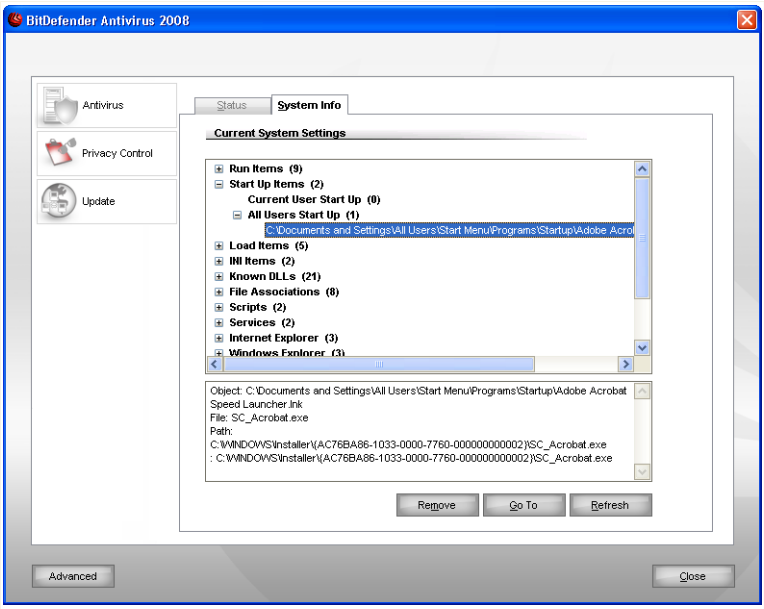
Click **Finish**.

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

8.6. 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.

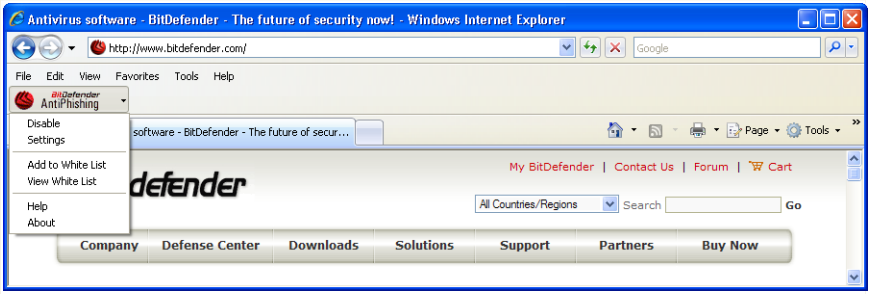
8.7. Antiphishing Toolbar

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.

9. 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:

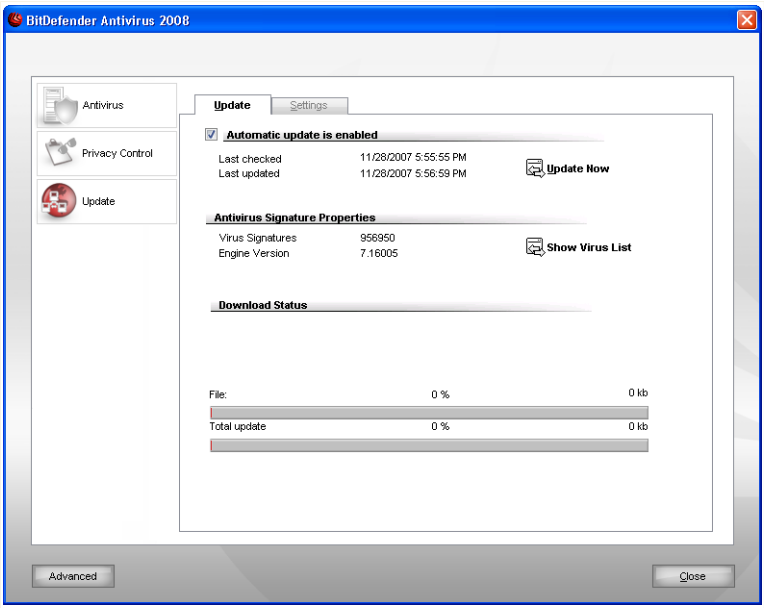
- **Updates for the antivirus engines** - as new threats appear, the files containing virus signatures must be updated to ensure permanent up-to-date protection against them. This update type is also known as **Virus Definitions Update**.
- **Updates for the antispam engines** - new rules will be added to the heuristic and URL filters and new images will be added to the Image filter. This will help increase the effectiveness of your Antispam engine. This update type is also known as **Antispam Update**.
- **Updates for the antispyware engines** - new spyware signatures will be added to the database. This update type is also known as **Antispyware Update**.
- **Product upgrades** - when a new product version is released, new features and scan techniques are introduced to the effect of improving the product's performance. This update type is also known as **Product Update**.

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

- Automatic Update
- Update Settings

9.1. 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.

9.1.1. 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**.

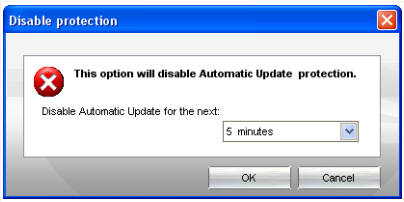
The **Update** module will connect to the BitDefender update server and will verify if any update is available. If an update was detected, depending on the options set in the Manual Update Settings section, you will be asked to confirm the update or the update will be made automatically.

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.

9.1.2. Disabling Automatic Update

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



Disable Automatic Update

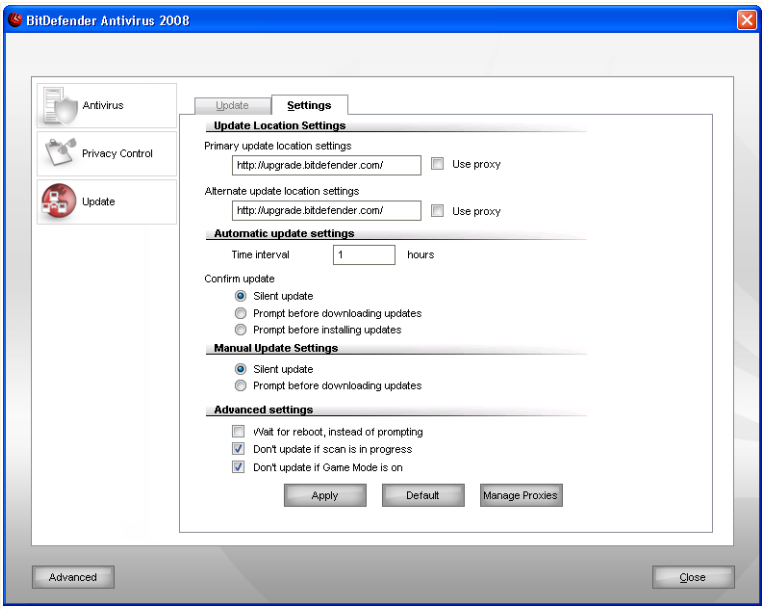
You must confirm your choice by selecting from the menu how long you want the automatic update to be disabled. You can disable the automatic update for 5, 15 or 30 minutes, for an hour, permanently or until the system restart.

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.

9.2. 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.

9.2.1. 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. 103)

9.2.2. 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.

9.2.3. 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.

9.2.4. 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.

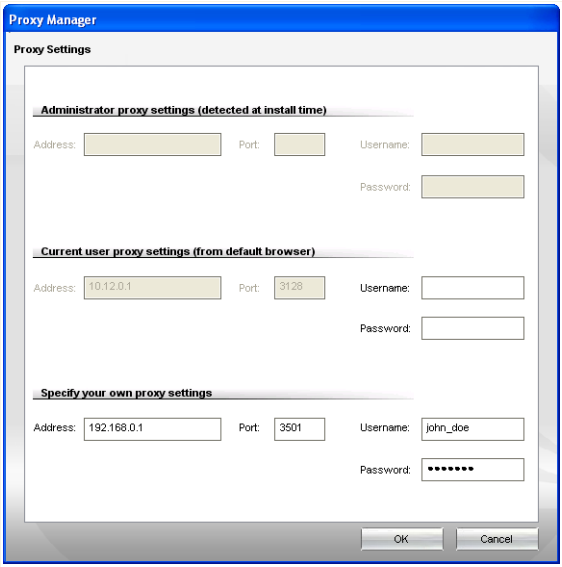
- **Don't update if game mode is on** - BitDefender will not update if the game mode is turned on. In this way, you can minimize the product's influence on system performance during games.

9.2.5. 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

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

10. Overview

BitDefender Antivirus 2008 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.

10.1. 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.

10.2. 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.

Iptraf

Iptraf is an IP Network Monitoring Software.

For more information, please refer to the Iptraf homepage.

Iftop

Iftop displays bandwidth usage on an interface.

For more information, please refer to the Iftop homepage.

MTR

MTR is a network diagnostic tool.

For more information, please refer to the MTR homepage.

PPPStatus

PPPStatus displays statistics about the incoming and outgoing TCP/IP traffic.

For more information, please refer to the PPPStatus homepage.

Wavemon

Wavemon is a monitoring application for wireless network devices.

For more information, please refer to the Wavemon homepage.

USBView

USBView displays information about devices connected to the USB bus.

For more information, please refer to the USBView homepage.

Pppconfig

Pppconfig helps automatically setting up a dial up ppp connection.

DSL/PPPoe

DSL/PPPoe configures a PPPoE (ADSL) connection.

I810rotate

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.

11. 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.

11.1. 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.

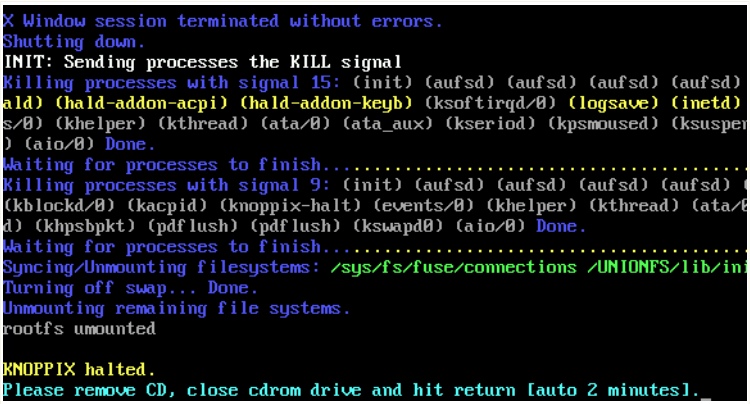
The Desktop

11.2. Stop BitDefender Rescue CD

You can safely shut down your computer by selecting **Exit** from the BitDefender Rescue CD contextual menu (right-click to open it) or by issuing the **halt** command in a terminal.

Choose "EXIT"

When BitDefender Rescue CD has successfully closed all programs it will show a screen like the following image. You may remove the CD in order to boot from your hard drive. Now it's ok to turn off your computer or to reboot it.



Wait for this message when shutting down

11.3. 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/
```

11.4. 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**.

11.5. 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:

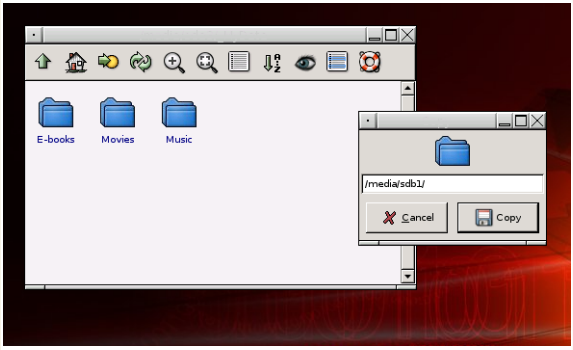
1. Put the BitDefender Rescue CD in the CD drive, the memory stick into the USB drive and then restart the computer.
2. Wait until BitDefender Rescue CD finishes booting. The following window will appear.

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

12. 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.

12.1. 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.

12.2. Asking for Help

12.2.1. Go to Web Self Service

Got a question? Our security experts are available to help you 24/7 via phone, email or chat at no additional cost.

Please, follow the links below:

English

http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2194/

German

http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2194/

French

http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2194/

Romanian

http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2194/

Spanish

http://www.bitdefender.com/es/KnowledgeBase/browseProducts/2194/

12.2.2. Open a support ticket

If you want to open a support ticket and receive help via email, just follow one of these links:

English: http://www.bitdefender.com/site/Main/contact/1/
German: http://www.bitdefender.de/site/Main/contact/1/
French: http://www.bitdefender.fr/site/Main/contact/1/
Romanian: http://www.bitdefender.ro/site/Main/contact/1/
Spanish: http://www.bitdefender.es/site/Main/contact/1/

12.3. 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.

12.3.1. 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

12.3.2. Local Distributor

The BitDefender local distributor is ready to respond to any inquiries regarding its area of operation, both in commercial and in general matters. Its address and contacts are listed below.

Australia

PICA Australia Pty Ltd
ABN 70 113 812 721
Australian BitDefender distributor
22 Aintree Street, Brunswick East Victoria
AUSTRALIA 3057
Tel: +61 3 9388 9588
Fax: +61 3 9388 9788
Sales: sales@pica.com.au

Web: http://www.pica.com.au
Technical Support: support@pica.com.au

12.3.3. Branch Offices

The BitDefender offices are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters. Their respective addresses and contacts are listed below.

Germany

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: soporte@bitdefender-es.com

Ventas: comercial@bitdefender-es.com
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Technical support: support@bitdefender.com
Customer Service: 954-776-6262
Web: http://www.bitdefender.com

Romania

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 it's own update module that allows you to manually check for updates, or let it automatically update the product.

Virus

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

Virus definition

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

Worm

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