BitDefender 8 Standard

User Guide

bitdefender
secure your every bit

Table of Contents

1

Terms of agreement

Software licensing

The BitDefender package is protected by the copyright law and the international treaties regarding the copyright, as well as other laws and treaties regarding the intellectual property.

The copyright law, as well as other intellectual property laws, protects in many countries the software owner's rights, according them some exclusive rights including the right to reproduce and copy the software. Copying the software without the owner's permission represents "copyright infringement" and the law imposes penalties and punishments.

Software is considered copied when:

- Loading the software in your computer's memory through running it from the floppy disk, hard disk, CD-ROM, or other media;
- Copying the software to another medium, such as floppy disk or hard disk;
- Running the program on the computer from a network server where the software is resident or deposited.

Almost any commercial software is directly or indirectly licensed to the copyright owner (the software developer) for final usage through a so-called licensing contract. The software products may have different types of licensing contracts.

BitDefender is a trademark of SOFTWIN. Microsoft, Windows, Excel, Word, and the Windows logo, Windows NT, and Windows 2000 are registered trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners.

License and warranty

IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS DO NOT INSTALL THE SOFTWARE. BY CLICKING "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.

This License Agreement is a legal agreement between you and SOFTWIN for use of the SOFTWIN software product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("BitDefender"), all of which are protected by U. S. and international copyright laws and international treaty protection. By installing, copying, or otherwise using BitDefender, you agree to be bound by the terms of this agreement.

If you do not agree to the terms of this agreement, do not install or use BitDefender; you may, however, return it to your place of purchase for a full refund within 30 days after your purchase. Verification of your purchase may be required.

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

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

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

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

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

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

UPGRADES. If BitDefender is labeled as an upgrade, you must be properly licensed to use a product identified by SOFTWIN as being eligible for the upgrade in order to use 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 have licensed as a single product, BitDefender may be used and transferred only as part of that single product package and may not be separated for use on more than one computer.

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

LIMITED WARRANTY. SOFTWIN warrants that the media on which BitDefender is distributed is free from defects for a period of thirty days from the date of delivery of BitDefender to you. Your sole remedy for a breach of this warranty will be that SOFTWIN, at its option, may replace the defective media upon receipt of the damaged media, or refund the money you paid for BitDefender. SOFTWIN does not warrant that BitDefender will be uninterrupted or error free or that the errors will be corrected. SOFTWIN does not warrant that BitDefender will meet your requirements.

SOFTWIN HEREBY DISCLAIMS ALL OTHER WARRANTIES FOR BITDEFENDER, WHETHER EXPRESSED OR IMPLIED. THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESSED OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

DAMAGES DISCLAIMER. Anyone using, testing, or evaluating BitDefender bears all risk to the quality and performance of BitDefender. In no event shall SOFTWIN be liable for any damages of any kind, including, without limitation, direct or indirect damages arising out of the use, performance, or delivery of BitDefender, even if SOFTWIN has been advised of the existence or possibility of such damages. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN NO CASE SHALL SOFTWIN'S LIABILITY EXCEED THE PURCHASE PRICE PAID BY YOU FOR BITDEFENDER. The disclaimers and limitations set forth above will apply regardless of whether you accept or use, evaluate, or test BitDefender.

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

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

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

2

BitDefender Rescue System

BitDefender 8 Standard comes with a bootable CD (**BitDefender Rescue System** based on **LinuxDefender**) capable to scan and disinfect all existing hard drives before your operating system starts.

You should use **BitDefender Rescue System** 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 System**.

System requirements

- Intel-compatible CPU (Pentium 2/300MHz or better);
- 64 MB of RAM for text mode, at least 256 MB for graphics mode with KDE (512 MB recommended);
- Standard SVGA-compatible graphics card.

How to scan

Steps to follow in order to scan your computer for viruses:

Boot from the CD

Insert the BitDefender rescue disk into your CD-ROM drive and restart the computer.

This will automatically launch the **BitDefender Rescue System** (you will probably need to set up the BIOS of your computer to boot off the CD; please refer to the User’s Manual of your motherboard for information on how to do that).

The **BitDefender Rescue System** desktop will appear:

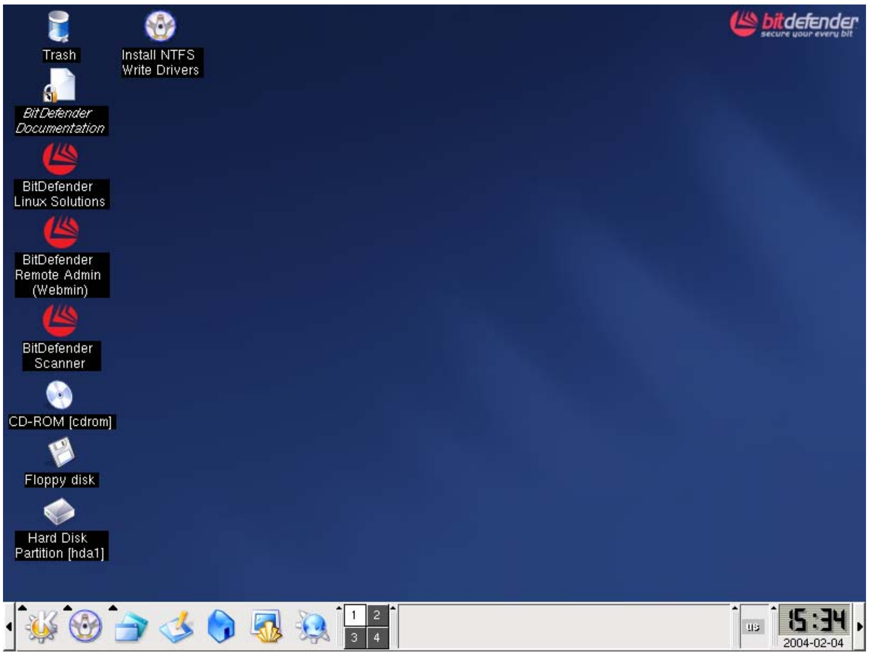

bitdefender
secure your every bit
Trash
Install NTFS Write Drivers
BitDefender Documentation
BitDefender Linux Solutions
BitDefender Remote Admin (Webmin)
BitDefender Scanner
CD-ROM [cdrom]
Floppy disk
Hard Disk Partition [hda1]
1 2 3 4
15:34
2004-02-04

Figure 1

Install the NTFS-driver

Click the **Install NTFS Write Drivers** icon using your left mouse key. In the window that will appear, click **Forward** twice. This will start the NTFS Driver installation. **BitDefender Rescue System** requires two drivers (`ntoskrnl.exe` and `ntfs.sys`) in order to read the files on your hard disk. Currently, only Windows XP drivers are supported. Note that you can use them to access Windows 2000/NT/2003 partitions too.

During the installation process you will receive the message:

`Cannot open target file "/var/lib/capative/ext2fsd.sys": Read-only file System`.

Confirm with **OK**. The installation will continue.

Click **Ok** to close the installation process.

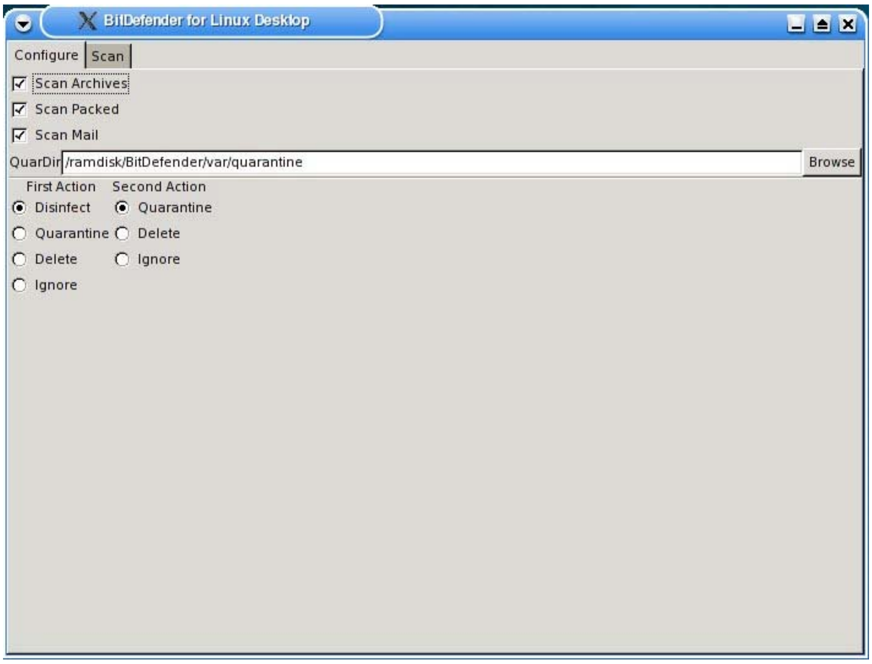
You will receive the message: `Although essential modules …`. Click **OK**.

Verify your hard disk

On the **BitDefender Rescue System** desktop, click **Hard Disk Partition [hda1]** icon. If the drivers were installed properly, clicking this icon will open a window that lists the contents of your hard disk. Close this window.

Select the scan options

Click the **BitDefender Scanner** icon to select the scan options. The following window will appear:



☑ Scan Archives
☑ Scan Packed
☑ Scan Mail

QuarDir /ramdisk/BitDefender/var/quarantine

First Action	Second Action
● Disinfect	● Quarantine
○ Quarantine	○ Delete
○ Delete	○ Ignore
○ Ignore	

Figure 2

The following options are available:

- **Scan Archives** - Scan inside archives.
- **Scan Packed** – Scan packed programs
- **Scan Mail** - Scan the mail database
- **QuarDir** – The default path to the quarantine folder is:

`/ramdisk/BitDefender/var/quarantine`. If you want to change the quarantine folder click **Browse** and select a different location (or you can type it in the **QuarDir** field).

BitDefender will try to perform an action if an infected file is found. You can select what action should be performed. If the first action fails for some reason, a second action (also configurable) will be taken.

TIP: We recommend using 1st action: **Disinfect**, 2nd action: **Delete**.

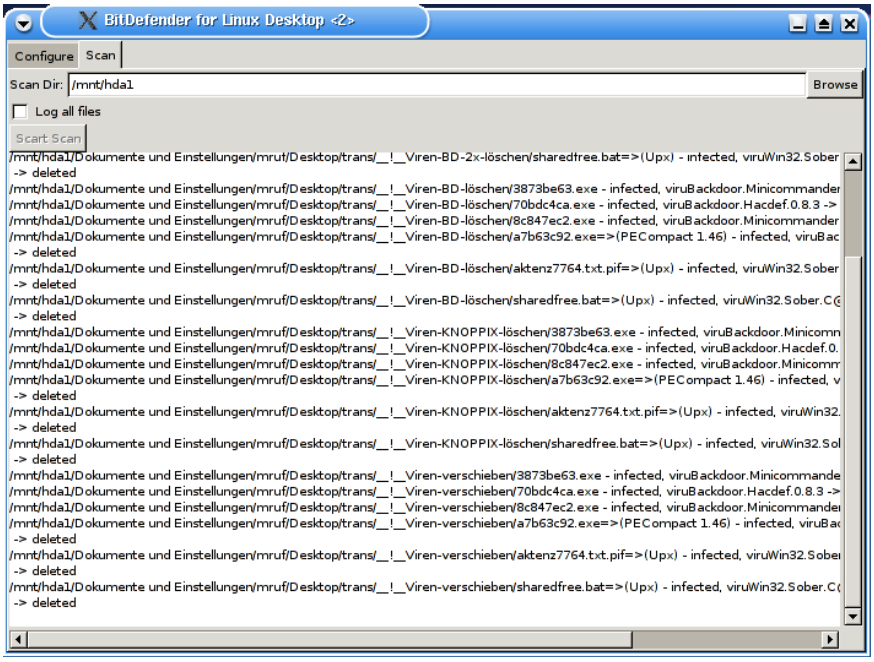
You can select one of the following actions:

First action	Description
Disinfect	Disinfect the infected files.
Quarantine	Move the infected files to the Quarantine folder. ! When you leave **BitDefender Rescue System**, the default quarantine folder will be deleted.
Delete	Delete the infected files immediately. You will not be prompted for confirmation.
Ignore	If an infected file is detected, it will be ignored.

Second action	Description
Quarantine	Move the infected files to the Quarantine folder.
Delete	Delete the infected files immediately. You will not be prompted for confirmation.
Ignore	If an infected file is detected, it will be ignored.

Start the scan process

Click the **Scan** tab.



Scan Dir: /mnt/hda1

□ Log all files

```
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-BD-2x-löschen/sharedfree.bat=>(Upx) - infected, viruWin32.Sober
 -> deleted
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-BD-löschen/3873be63.exe - infected, viruBackdoor.Minicommander
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-BD-löschen/70bdc4ca.exe - infected, viruBackdoor.Hacdef.0.8.3 ->
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-BD-löschen/8c847ec2.exe - infected, viruBackdoor.Minicommander
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-BD-löschen/a7b63c92.exe=>(PECompact 1.46) - infected, viruBac
 -> deleted
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-BD-löschen/aktenz7764.txt.pif=>(Upx) - infected, viruWin32.Sober
 -> deleted
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-BD-löschen/sharedfree.bat=>(Upx) - infected, viruWin32.Sober.C@
 -> deleted
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-KNOPPIX-löschen/3873be63.exe - infected, viruBackdoor.Minicomn
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-KNOPPIX-löschen/70bdc4ca.exe - infected, viruBackdoor.Hacdef.0.
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-KNOPPIX-löschen/8c847ec2.exe - infected, viruBackdoor.Minicomm
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-KNOPPIX-löschen/a7b63c92.exe=>(PECompact 1.46) - infected, v
 -> deleted
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-KNOPPIX-löschen/aktenz7764.txt.pif=>(Upx) - infected, viruWin32.
 -> deleted
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-KNOPPIX-löschen/sharedfree.bat=>(Upx) - infected, viruWin32.Sol
 -> deleted
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-verschieben/3873be63.exe - infected, viruBackdoor.Minicommande
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-verschieben/70bdc4ca.exe - infected, viruBackdoor.Hacdef.0.8.3 ->
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-verschieben/8c847ec2.exe - infected, viruBackdoor.Minicommande
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-verschieben/a7b63c92.exe=>(PECompact 1.46) - infected, viruBa
 -> deleted
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-verschieben/aktenz7764.txt.pif=>(Upx) - infected, viruWin32.Sobe
 -> deleted
/mnt/hda1/Dokumente und Einstellungen/mruf/Desktop/trans/__!__Viren-verschieben/sharedfree.bat=>(Upx) - infected, viruWin32.Sober.C(
 -> deleted
```

Figure 3

In the **Scan Dir** field you must specify the path to the hard disk you want to scan.

Examples:

If you have one hard disk with 3 partitions, you must scan each partition separately.

- `/mnt/hda1` – for the first partition;
- `/mnt/hda2` – for the second partition;
- `/mnt/hda3` – for the third partition.

If you have a second hard disk with two partitions the syntax is:

- `/mnt/hdb1`– for the first partition;
- `/mnt/hdb2`– for the second partition.

If you are using a SCSI hard disk with two partitions the syntax is:

- `/mnt/sda1`– for the first partition;
- `/mnt/sda2`– for the second partition.

The option **Log all files** is left unchecked by default, because the scan process would take a very long time otherwise.

Click **Start Scan**. This will start the scanning process.

When a virus is found, BitDefender will inform you by displaying a message in the main window.

Note

Please perform the virus scan twice. Some viruses cannot be removed the first time you scan a NTFS partition.

3

Product installation

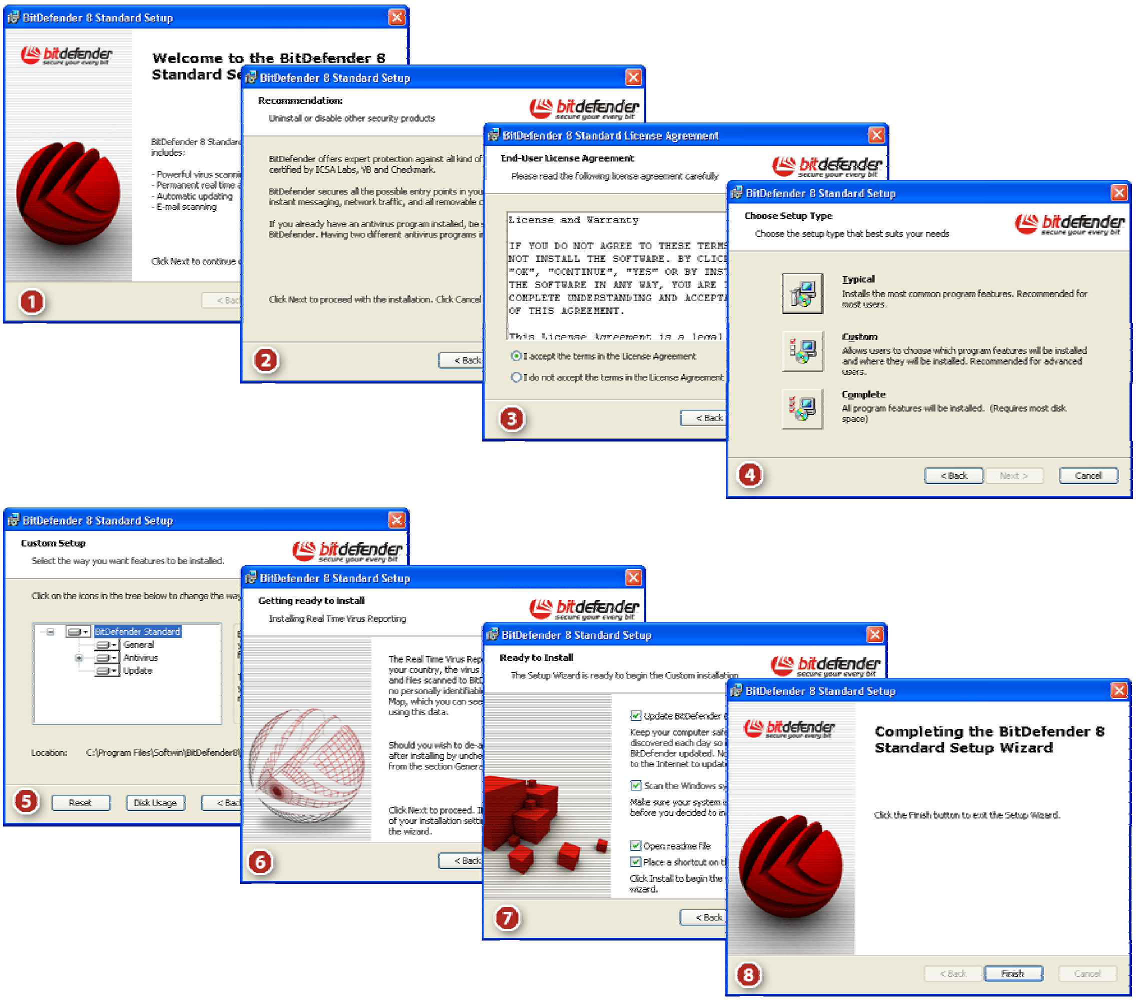
System requirements

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

Minimum Processor: Pentium 200MHz
Minimum hard disk space: 40MB
Minimum RAM Memory: 64MB (128MB Recommended)
Operating system: Windows 98/NT-SP6/ME/2000/XP; Internet Explorer 4.0 (+)

Installation steps

Locate the setup file and double click with the mouse on it. This will launch the setup wizard, which will guide you through the setup process.



BitDefender 8 Standard Setup

Welcome to the BitDefender 8 Standard Se

BitDefender 8 Standar includes:

- Powerful virus scanni
- Permanent real time
- Automatic updating
- E-mail scanning

Click Next to continue

BitDefender 8 Standard Setup

Recommendation:

Uninstall or disable other security products

BitDefender offers expert protection against all kind of certified by ICSA Labs, VB and Checkmark.

BitDefender secures all the possible entry points in you instant messaging, network traffic, and all removable c

If you already have an antivirus program installed, be BitDefender. Having two different antivirus programs i

Click Next to proceed with the installation. Click Cancel

BitDefender 8 Standard License Agreement

End-User License Agreement

Please read the following license agreement carefully

License and Warranty

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

This License Agreement is a legal

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

BitDefender 8 Standard Setup

Choose Setup Type

Choose the setup type that best suits your needs

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

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

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

BitDefender 8 Standard Setup

Custom Setup

Select the way you want features to be installed.

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

BitDefender Standard
General
Antivirus
Update

Location: C:\Program Files\Softwin\BitDefender8\

BitDefender 8 Standard Setup

Getting ready to install

Installing Real Time Virus Reporting

The Real Time Virus Rep your country, the virus and files scanned to Bit no personally identifiab Map, which you can see using this data.

Should you wish to de-a after installing by unche from the section Genera

Click Next to proceed. I of your installation setti the wizard.

BitDefender 8 Standard Setup

Ready to Install

The Setup Wizard is ready to begin the Custom installation

☑ Update BitDefender
Keep your computer safe discovered each day so BitDefender updated. N to the Internet to updat

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

☑ Open readme file

☑ Place a shortcut on t

Click Install to begin the wizard.

BitDefender 8 Standard Setup

Completing the BitDefender 8 Standard Setup Wizard

Click the Finish button to exit the Setup Wizard.

Figure 4

Installation steps:

1. Click **Next** to continue or click **Cancel** if you want to quit installation.
2. Click **Next** to continue or click **Back** to return to the first step.
3. Please read the **License Agreement**, select **I accept the terms in the License Agreement** and click **Next**. If you do not agree with these terms click **Cancel**. The installation process will be abandoned and you will exit setup.
4. You can choose what kind of installation you want: typical, custom or complete.
   - **Typical** – The program will be installed with the most common options. This is the recommended option for most users.
   - **Custom** – You may choose the components you want to install. Recommended for advanced users only.
   - **Complete** – For full installation of the product. All BitDefender modules will be installed.

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

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

You can select the folder where you want to install the product. The default folder is `C:\Program Files\Softwin\BitDefender 8`.

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

6. Click **Next**.
7. You have four options selected by default:

   ➔ **Update BitDefender** – to update BitDefender at the end of the installation. Your system must be connected to the Internet to update.
   ➔ **Run a full system scan** – to scan the entire computer for viruses at the end of the installation.
   ➔ **Open readme file** – to open the readme file at the end of the installation.
   ➔ **Place a shortcut on the desktop** – to place a shortcut to BitDefender on your desktop at the end of the installation.

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

Note

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

Removing, repairing or modifying BitDefender features

If you want to modify, repair or remove **BitDefender 8 Standard**, follow the path from the Windows start menu: **Start** → **Programs** → **BitDefender 8** → **Modify, Repair or Uninstall**.

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

- **Modify** – to select new program components to add or to select currently installed components to remove.
- **Repair** – to re-install all program components installed by the previous setup.
- **Remove** – to remove all installed components.

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

4

Description and features

Description

BitDefender Standard Edition is a powerful antivirus tool with features that best meet your security needs. Ease of use and automatic updating make **BitDefender Standard Edition** an "install and forget" antivirus product.

Main Features

BitDefender 8 Standard includes 2 protection modules: **Antivirus** and **Update**.

Antivirus

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

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

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

Innovative Behavior Blocking
Blocks malicious applications based on behavior analysis. The method ensures proactive protection against newborn viruses, Trojans, Internet worms and other potentially malicious codes. The file system, registry and Internet activity are constantly monitored.

Quarantine zone

Suspicious/infected files can optionally be backed up into a safe quarantine area before being disinfected or deleted. The contents of the quarantine can be sent to BitDefender Labs, for detailed analysis. Files that proved harmless can be easily moved out of quarantine, back to their original place.

Full e-mail protection

The application runs on the POP3 protocol level, blocking any infected e-mail message, regardless of the e-mail client used (MS Exchange, MS Outlook, MS Outlook Express, Netscape, Eudora, Lotus Notes, Pegasus, The Bat, etc), without any additional configuration.

Update

This is the module that performs the update of the product, with new virus signatures and new features.

Fast, Free Updates

Intelligently updates the antivirus protection, without user's intervention. Update can be performed from the network, over the Internet, directly or through a Proxy Server. BitDefender license owners benefit from free virus signatures update and free product upgrades.

Self-repairing

The product is able to repair itself if necessary, by downloading the damaged or missing files from BitDefender servers.

Automated Update

Updates to the Antivirus engines are free and fully automated. Checks for updates can be scheduled to take place as often as necessary.

Other Features

Informed Decisions

Configuration wizards are at hand to step you through all the procedures you need to follow to secure your system. A comprehensive “trusted apps” database holds data on whether the applications demanding network access are trustworthy, so you can make informed decisions.

Easy to Install and to Use

A friendly interface makes it easier for you to install and use the product. The intuitive Scan activity bar tool lets you drag and drop files to scan them.

24/7 Hours Professional Technical Support

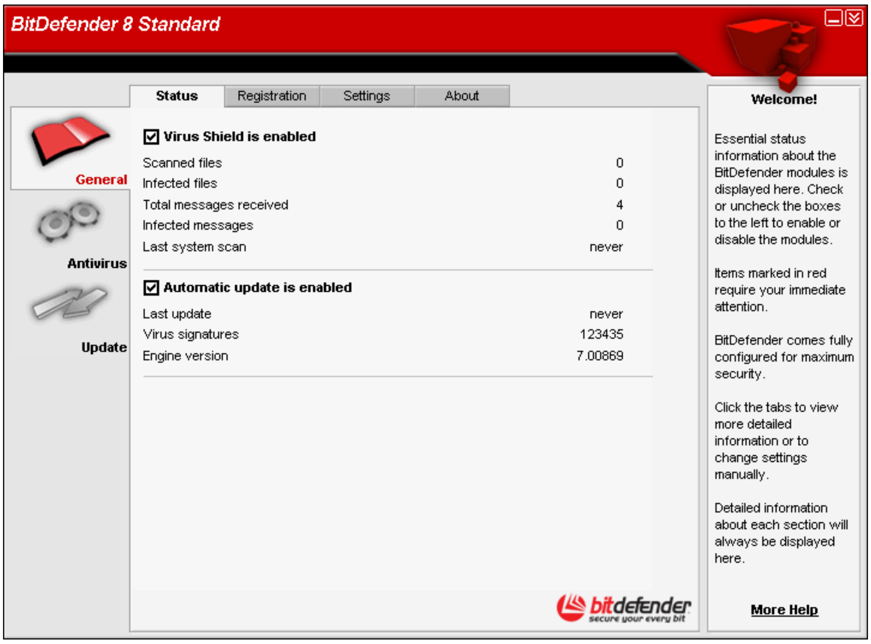
Offered by qualified support representatives and an online database with answers to Frequently Asked Questions.

The Management Console

General view

BitDefender 8 Standard was designed with a centralized management console, which allows the configuration of the protection options for all BitDefender modules. In other words, it is enough to open the management console in order to have access to all modules: **Antivirus** and **Update**.

To access the management console, use the Windows Start menu, by following the path **Start** → **Programs** → **BitDefender 8** → **BitDefender 8 Standard** or quicker, double click the BitDefender icon from the system tray.



☑ **Virus Shield is enabled**

Scanned files	0
Infected files	0
Total messages received	4
Infected messages	0
Last system scan	never

☑ **Automatic update is enabled**

Last update	never
Virus signatures	123435
Engine version	7.00869

Welcome!

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

Items marked in red require your immediate attention.

BitDefender comes fully configured for maximum security.

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

Detailed information about each section will always be displayed here.

Figure 5

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

- ➔ General – to access the section where you can see a summary of all the BitDefender main settings, product details and contact information. Here you can also register the product.
- ➔ Antivirus – to access the antivirus configuration window.
- ➔ Update – to access the product update configuration window.

The option **More Help**, placed at the right bottom, opens the **Help** file.

When the console is minimized, an icon will appear in the system tray (*Figure 6*).

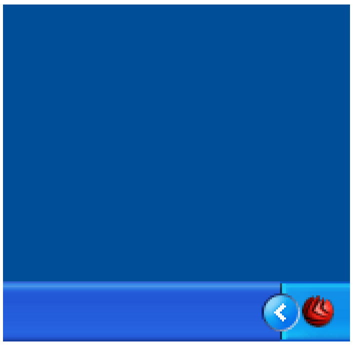


Figure 6

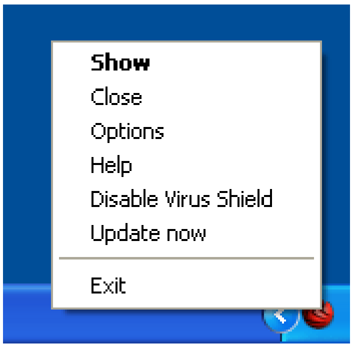


Figure 7

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

Also, by right-clicking it, a pop menu, as in *Figure 7*, containing the following options, will appear.

- ➔ **Show** – opens the management console.
- ➔ **Close** – minimizes the management console to system tray.
- ➔ **Options** – opens a window with the options for the management console.
- ➔ **Help** - opens the electronic documentation.
- ➔ **Enable** / **Disable Virus Shield** – enables / disables Virus Shield.
- ➔ **Update now** – performs an immediate update.
- ➔ **Exit** – shuts down the application. By selecting this option, the icon from the system tray will disappear and in order to access the management console, you will have to launch it again from the Start menu.

Note

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

Scan activity bar

Many of you have probably been puzzled by the “little gray rectangle” that can be moved in any corner of the screen.

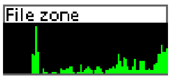


Figure 8

This window is a graphic visualization of the scanning activity on your system.

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

Note

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

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

TIP: To completely hide this window, uncheck **Show Scan Activity Bar** option (from the **Antivirus** module, Shield section).

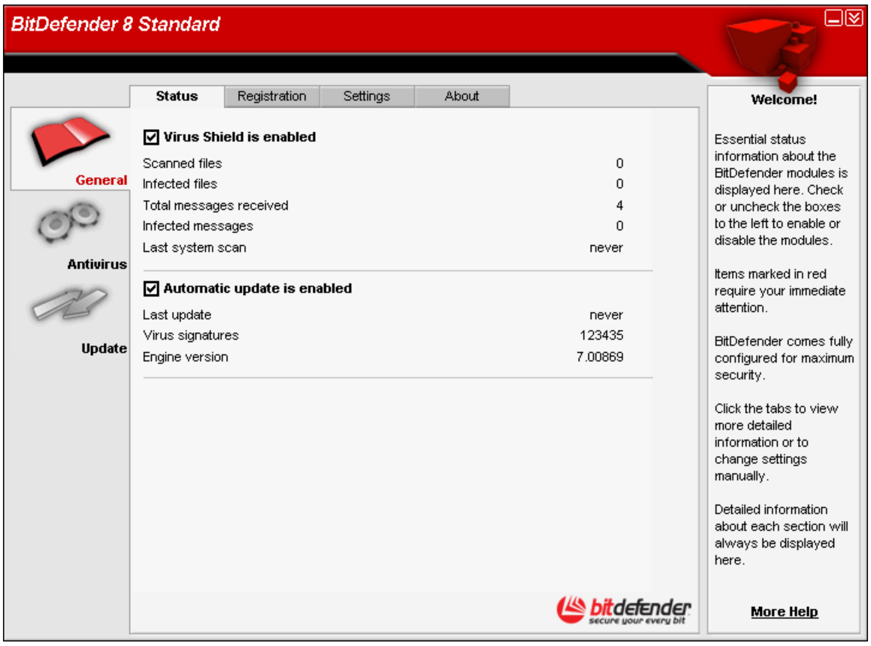
General module

BitDefender comes fully configured for maximum security. Essential status information about all the BitDefender modules is displayed in the **General** module.

The **General** module contains 4 different sections: Status, Registration, Settings and About.

Status

Here you can review information regarding the product status.



☑ Virus Shield is enabled

```
Scanned files                 0
Infected files                0
Total messages received       4
Infected messages             0
Last system scan          never
```

☑ Automatic update is enabled

```
Last update               never
Virus signatures         123435
Engine version          7.00869
```

Welcome!

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

Items marked in red require your immediate attention.

BitDefender comes fully configured for maximum security.

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

Detailed information about each section will always be displayed here.

Figure 9

By setting or removing the mark in the checkboxes, you can enable or disable the main features of BitDefender.

Items marked in red require your immediate attention.

Virus Shield

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

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

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

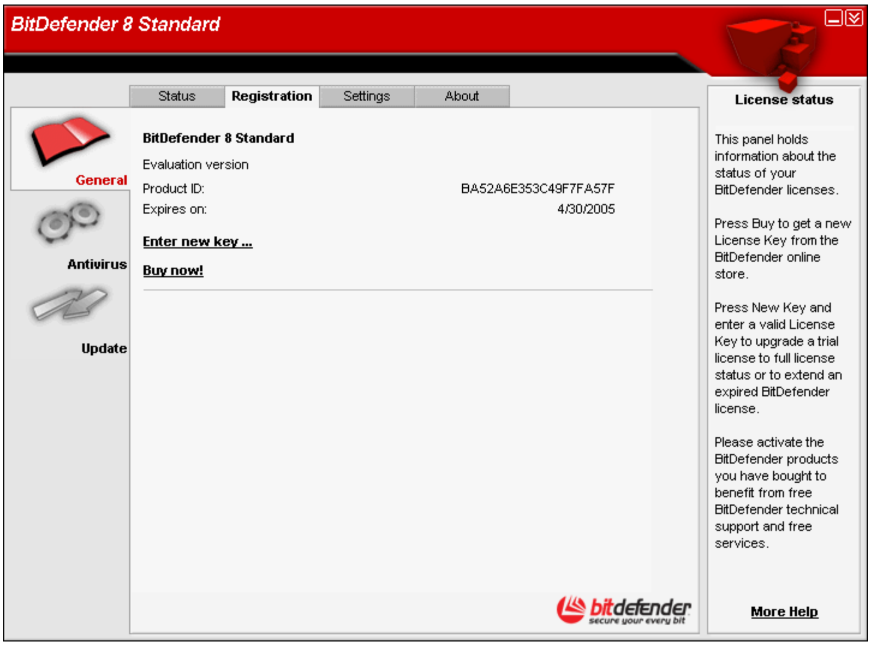
Automatic Update

New viruses are found and identified every day. This is why it is very important to keep BitDefender up to date with the latest virus signatures. It displays the date of the last update and the number of viruses that can be detected (and therefore disinfected) from your BitDefender database.

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

Product registration

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



BitDefender 8 Standard

Evaluation version

Product ID: BA52A6E353C49F7FA57F

Expires on: 4/30/2005

Enter new key ...

Buy now!

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

Press Buy to get a new License Key from the BitDefender online store.

Press New Key and enter a valid License Key to upgrade a trial license to full license status or to extend an expired BitDefender license.

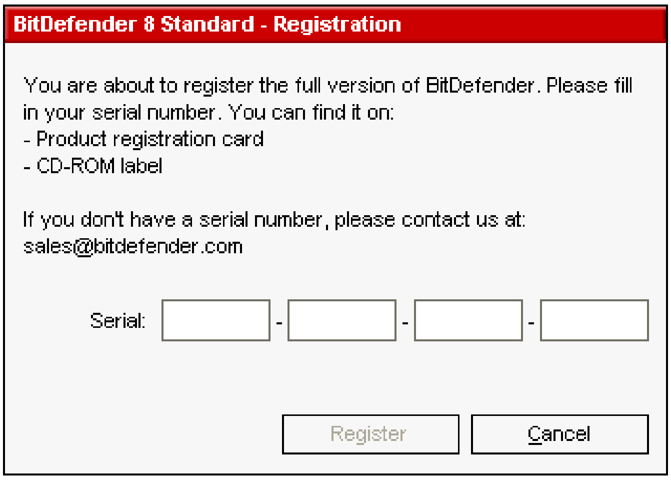
Please activate the BitDefender products you have bought to benefit from free BitDefender technical support and free services.

Figure 10

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

To modify the default license key click **Enter new key**.

The following window will open:



BitDefender 8 Standard - Registration

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

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

Serial: [ ] - [ ] - [ ] - [ ]

Figure 11

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

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

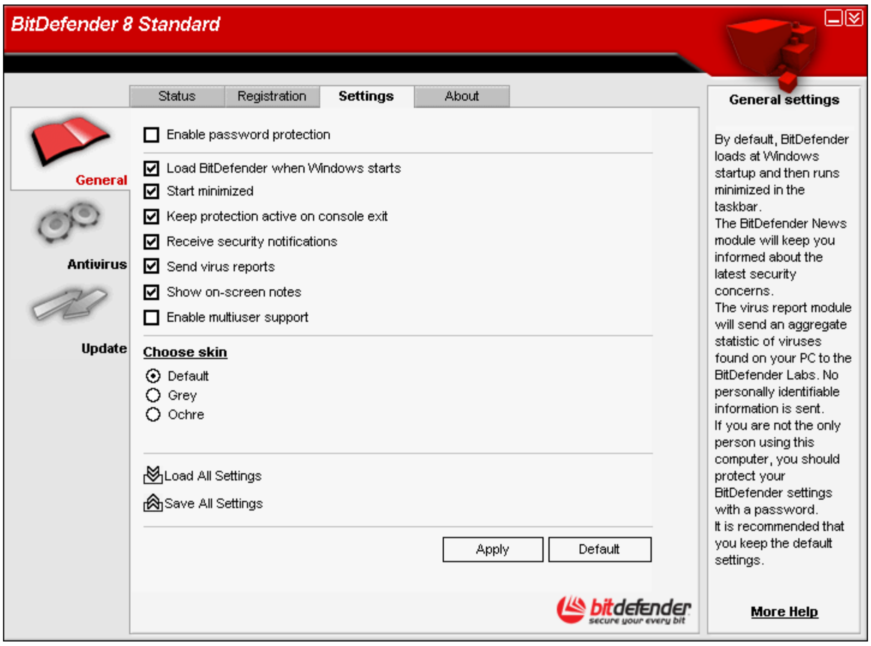
If you type in a valid license key a success message box appears.

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

TIP: Please activate the BitDefender products you have bought to benefit from BitDefender technical support and free services.

Management console settings

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



BitDefender 8 Standard

☐ Enable password protection

☑ Load BitDefender when Windows starts

☑ Start minimized

☑ Keep protection active on console exit

☑ Receive security notifications

☑ Send virus reports

☑ Show on-screen notes

☐ Enable multiuser support

Choose skin

● Default

○ Grey

○ Ochre

General settings

By default, BitDefender loads at Windows startup and then runs minimized in the taskbar.
The BitDefender News module will keep you informed about the latest security concerns.
The virus report module will send an aggregate statistic of viruses found on your PC to the BitDefender Labs. No personally identifiable information is sent.
If you are not the only person using this computer, you should protect your BitDefender settings with a password.
It is recommended that you keep the default settings.

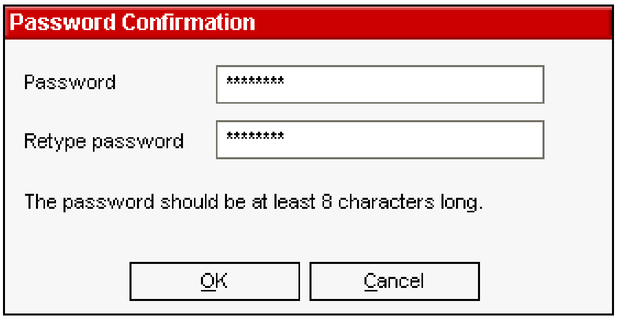
Figure 12

To select an option, just click with the mouse on the corresponding checkbox.

➔ **Enable password protection** – enables setting a password in order to protect the BitDefender configuration.

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

The next window will appear:



Password Confirmation

Password ********

Retype password ********

The password should be at least 8 characters long.

Figure 13

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

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

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

- **Load BitDefender when Windows starts** – automatically launches BitDefender at system startup. This is highly recommended!

- **Start minimized** – minimizes the BitDefender management console after it has been loaded at system startup. Only the BitDefender icon will appear in the system tray.

- **Keep protection active on console exit** – even when the management console is closed (from the system tray too), BitDefender continuously protects you.

- **Receive security notifications** - receives from time to time security notifications regarding virus outbreaks, sent by the BitDefender server.

- **Show splash screen** – shows the screen that appears when you launch BitDefender.

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

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

- **Show on-screen notes** – shows pop-up windows regarding the product status.

- **Enable multiuser support** – allows other users that may be using this computer to have their own settings for BitDefender.

Note

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

- The **Skin file** option allows you to select the color of the management console. The skin represents the background image on the interface. In order to select a different skin, click the corresponding color.

At the end, click **Apply** to save the changes.

About

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

BitDefender^{TM} provides security solutions to satisfy the protection requirements of today's computing environment, delivering effective threat management for over 38 million home and corporate users in more than 100 countries.

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

Antivirus module

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

More features

From the antivirus module you have access to all BitDefender antivirus settings and features.

On-access scanning and On-demand scanning

Virus protection is divided into two categories:

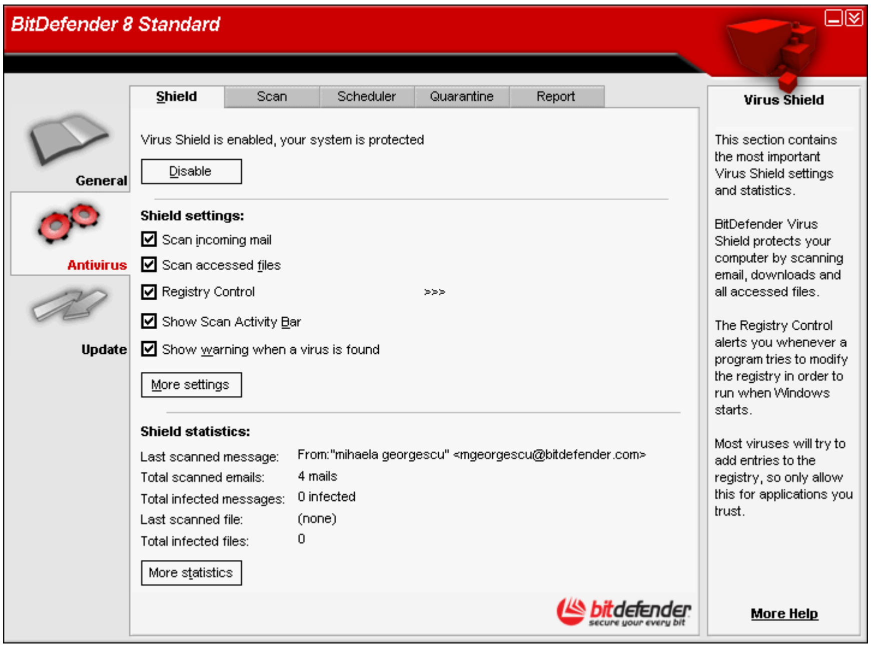
- On-access scanning: Prevents new viruses from entering your system. This is also called a virus shield - Files are scanned as the user accesses them. BitDefender will, for example, scan a word document for viruses when you open it, and an e-mail message when you receive one. BitDefender scans "as you use your files" - on-access.
- On-demand scanning: Detects already resident viruses in your system. This is the classic virus-scan initiated by the user - you choose what drive, folder or file BitDefender should scan, and BitDefender scans it - on-demand.

More detailed explanations of these types of scanning are presented further.

On access scanning

In case you haven't already opened the management console, you can access it from the Windows Start menu, following the path **Start** → **Programs** → **BitDefender** → **BitDefender 8 Standard** or quicker, double click the BitDefender icon from the system tray.

In the management console, click **Antivirus**.



Virus Shield is enabled, your system is protected

Disable

Shield settings:

☑ Scan incoming mail
☑ Scan accessed files
☑ Registry Control >>>
☑ Show Scan Activity Bar
☑ Show warning when a virus is found

More settings

Shield statistics:

Last scanned message:	From:"mihaela georgescu" <mgeorgescu@bitdefender.com>
Total scanned emails:	4 mails
Total infected messages:	0 infected
Last scanned file:	(none)
Total infected files:	0

More statistics

Virus Shield

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

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

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

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

More Help

Figure 14

The **Virus Shield** protects your computer by scanning e-mail messages, downloads and all accessed files.

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

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

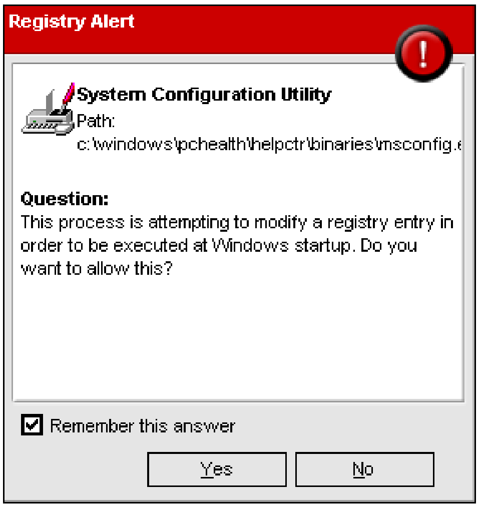
With the settings you can customize what BitDefender should scan on-access and how it should react if it encounters a virus.

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
System Configuration Utility
Path:
c:\windows\pchealth\helpctr\binaries\msconfig.e
☑ Remember this answer
Yes
No

Question:
This process is attempting to modify a registry entry in order to be executed at Windows startup. Do you want to allow this?

Figure 15

You can deny this modification by clicking **No** or you can allow it by clicking **Yes**. If you want BitDefender to remember your answer you must select the checkbox: **Remember this answer**.

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

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

The following window will appear:

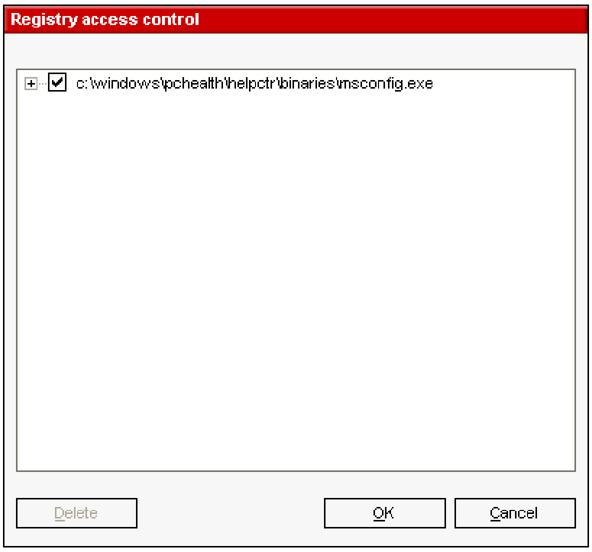


Figure 16

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

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

To temporarily deactivate a registry entry without deleting it, clear the check mark from the box beside it ☑ by clicking it. When the registry entry is deactivated the box will look like this □.

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.

Select the most important settings

To select an option, just click with the mouse on the corresponding check box:

- **Scan incoming email** – all the incoming e-mail messages will be scanned by BitDefender. This is highly recommended!

- **Scan accessed files** – all the accessed files will be scanned by BitDefender.

- **Show warning when a virus is found** – an alert window will be displayed when a virus is found in a file or in an e-mail message.

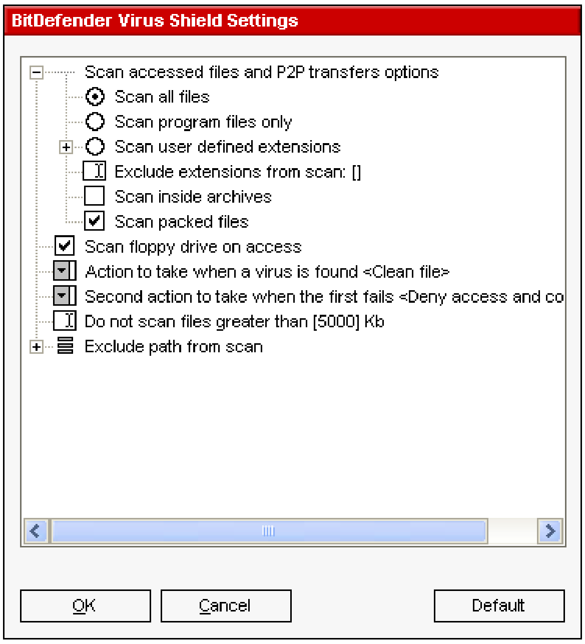
  For an infected file the alert window will contain the name of the virus, the path to it, the action taken by Bitdefender and a link to the BitDefender site where you can find more information about it. For an infected e-mail the alert window will contain also information about the sender and the receiver.

  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.

- **Show Scan Activity Bar** – deselect this option if you no longer want to see the scan activity bar.

Select other options

Click **More settings** to select the object you want to scan and the action to take on the infected files. The following window will appear:



BitDefender Virus Shield Settings

```
⊟ Scan accessed files and P2P transfers options
    ● Scan all files
    ○ Scan program files only
  ⊞ ○ Scan user defined extensions
    ☐ Exclude extensions from scan: []
    ☐ Scan inside archives
    ☑ Scan packed files
  ☑ Scan floppy drive on access
  ▾ Action to take when a virus is found <Clean file>
  ▾ Second action to take when the first fails <Deny access and co
  ☐ Do not scan files greater than [5000] Kb
⊞ Exclude path from scan
```

Figure 17

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

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

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

The following options are available:

Option	Description
Scan all files	All the accessed files will be scanned, regardless their type.
Scan program files only	Only the program files will be scanned. This means only the files with the following extensions: `exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; 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; pfd; msi; ini; csc; cmd; bas; eml; nws.`
Scan user defined extensions	Only the files with the extensions specified by the user will be scanned. These extensions must be separated by ";".
Exclude extensions from scan	The files with the extensions specified by the user will NOT be scanned. These extensions must be separated by ";".
Scan inside archives	Also the accessed archives will be scanned.
Scan packed files	All packed files will be scanned.

➔ Select **Scan floppy drive on access** if you wish to scan the floppy drive, when it is accessed.

➔ Click the arrow corresponding to **Action to take when a virus is found** and select from the list the first action on infected files.

BitDefender allows selecting two actions in case an infected file is found. The second action is enabled only in case the first action you selected is to disinfect the infected files.

You can select one of the following actions:

Action	Description
Deny access and continue	In case an infected file is detected, the access to this will be denied.
Clean file	To disinfect the infected file.
Delete file	Deletes the infected files immediately, without any warning.
Move to quarantine	The infected files are moved into quarantine. When the virus is in quarantine it can't do any harm.

➔ Click the arrow corresponding to **Second action to take when first fails** and select from the list the second action on the infected files.

The following options are available.

Action	Description
Deny access and continue	In case an infected file is detected, the access to this will be denied.
Clean file	To disinfect the infected file.
Delete file	Deletes the infected files immediately, without any warning.
Move to quarantine	The infected files are moved into quarantine. When the virus is in quarantine it can't do any harm.

➔ Click **Do not scan files greater than** and type in the maximum size of the files to be scanned. If the size is 0 Kb, all files will be scanned.

➔ Click "+" corresponding to **Exclude path from scan** in order to specify a folder that will be excluded from scanning. The consequence of this will be that the option will expand and a new option, **New item**, will appear. Click the corresponding box of the new item and from the exploring window select the folder you want to be excluded from scanning.

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

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.

BitDefender allows four types of on demand scan:

- Immediate scanning – there are a few steps to follow in order to scan your computer for viruses;
- Contextual scanning – right-click on a file or a folder and select **BitDefender Antivirus v8**;
- Drag & Drop scanning – drag & drop a file or a folder over the Scan Activity Bar;
- Scheduled scanning – you can program BitDefender to scan your system for viruses periodically.

Immediate scanning

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

1. Close all open programs

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

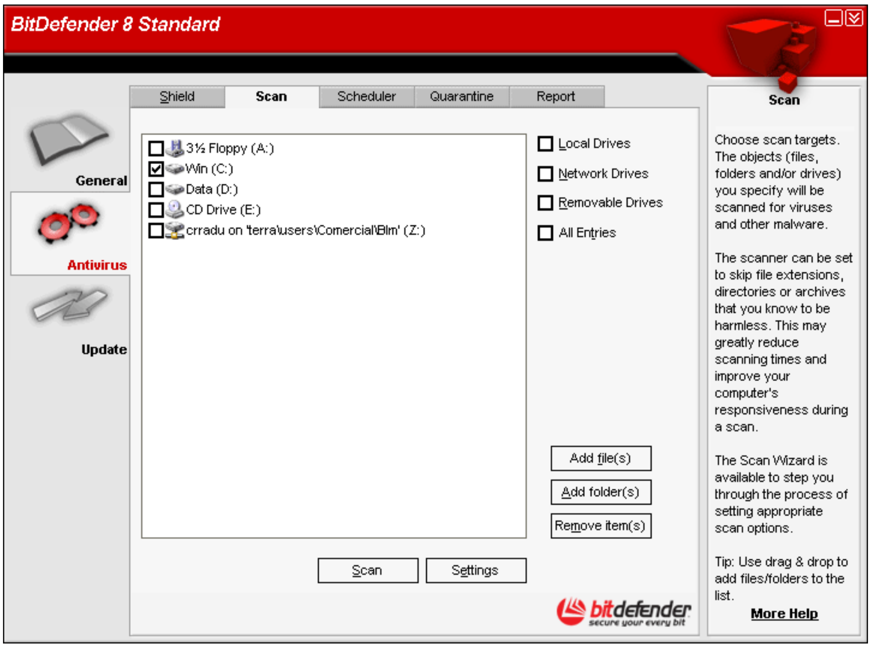
2. Make sure that BitDefender knows the latest viruses

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

If this date is not recent, you should let BitDefender update its virus signatures. This is very easy, and all you have to do is to click the **Check** button from the Update module.

3. Choose scan targets

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



☐ 3½ Floppy (A:)
☑ Win (C:)
☐ Data (D:)
☐ CD Drive (E:)
☐ crradu on 'terra\users\Comercial\Blm' (Z:)

☐ Local Drives
☐ Network Drives
☐ Removable Drives
☐ All Entries

Scan

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

The scanner can be set to skip file extensions, directories or archives that you know to be harmless. This may greatly reduce scanning times and improve your computer's responsiveness during a scan.

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

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

Figure 18

The section contains the following buttons:

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

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

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

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

- **Settings** – opens a window where you can specify which files to be scanned, the action on the infected files, generating alert messages, saving scan results in report files.
- **Scan** - launches the system scanning, taking in account the selected scan options.

Options that allow the fast selection of the scan locations:

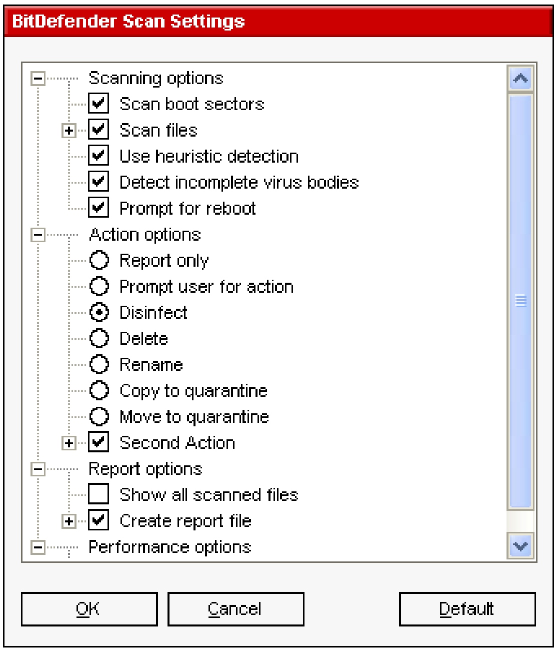
- **Local drives** – to scan the local drives.
- **Network drives** – to scan all network drives.
- **Removable drives** – to scan the removable drives (CD-ROM, floppy-disk unit).
- **All entries** – to scan all drives, no matter if they are local, in the network or removable.

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

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

4. Select the scan options – only for advanced users

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



BitDefender Scan Settings

- Scanning options
  - ☑ Scan boot sectors
  - ☑ Scan files
  - ☑ Use heuristic detection
  - ☑ Detect incomplete virus bodies
  - ☑ Prompt for reboot
- Action options
  - ○ Report only
  - ○ Prompt user for action
  - ● Disinfect
  - ○ Delete
  - ○ Rename
  - ○ Copy to quarantine
  - ○ Move to quarantine
  - ☑ Second Action
- Report options
  - □ Show all scanned files
  - ☑ Create report file
- Performance options

Figure 19

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

The scan options are grouped in four categories:

- **Scanning options**
- **Action options**
- **Report options**
- **Performance options**

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

The following step is to specify the type of objects to be scanned (archives, e-mail messages and so on) and enabling heuristic scan (for detecting unknown viruses). This is made through the selection of certain options from **Detection options** category. The following detection options are available:

Option		Description
Scan boot sectors		To scan the system's boot sector.
Scan files	Scan all files	To scan all files regardless of their type.
	Scan program files only	To scan only the program files. 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; 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; pfd; msi; ini; csc; cmd; bas; eml; nws.`
	Scan user defined extensions	To scan only the files with the extensions specified by the user. These extensions must be separated by ";".
	Exclude user defined extensions	To scan all files, except the ones with the extensions indicated by the user. These extensions must be separated by ";".
	Open packed programs	To scan packed files.
	Open archives	To scan inside archives.
	Open mails	To scan inside mail archives.

Option	Description
Use heuristic detection	To use heuristic scanning of the files. The aim of heuristic scanning is to identify new viruses, based on certain patterns and algorithms, before a virus definition is found. False alarm messages can appear. When such a file is detected it is classified as suspicious. In these cases, we recommend you to send the file to the BitDefender lab to be analyzed.
Detect incomplete virus bodies	To detect incomplete virus bodies too.

Further on, you'll have to specify the action on infected or suspicious files. Click the "+" sign corresponding to **Action options** in order to open the option and see all possible actions on infected files.

You can select one of the following:

Action	Description
Report only	To report the detection of an infected file and the virus name.
Prompt user for action	When an infected file is detected, a window will appear prompting the user to select the action on that file. Depending on the importance of that file, you can select to disinfect it, isolate it in the quarantine zone or delete it.
Disinfect	To disinfect the infected files.
Delete	To delete infected files.
Rename	To change the extension of the infected files. The new extension of the infected files will be `.vir`. By renaming the infected files, the possibility of executing and thus of spreading the infection is removed. At the same time they can be saved for further examination and analysis.
Copy to quarantine	To copy the infected files in the quarantine zone. ❗ This means practically duplicating the infected file and the copy of this file will appear in the quarantine, but the infected file will not be moved from the initial location.
Move to quarantine	To move to the quarantine zone the infected files. ❗ When the virus is in quarantine it can't do any harm.
Second action	Check this option if you want to select the second action to take on infected files.

To select the second action on infected files, click the corresponding "+"sign, after you have previously checked **Second action**. The options available for the second action are described in the below table.

Action	Description
Report only	To report the detection of an infected file and the virus name.
Prompt user for action	When an infected file is detected, a window will appear prompting the user to select the action on that file. Depending on the importance of that file, you can select to disinfect it, isolate it in the quarantine zone or delete it.
Delete	To delete infected files.

Action	Description
Rename	To change the extension of the infected files. The new extension of the infected files will be `.vir`. By renaming the infected files, the possibility of executing and thus of spreading the infection is removed. At the same time they can be saved for further examination and analysis.
Copy to quarantine	To copy the infected files in the quarantine zone, from where they can be send to the BitDefender lab to be analyzed. This means practically duplicating the infected file and the copy of this file will appear in the quarantine, but the infected file will not be moved from the initial location.
Move to quarantine	To move to the quarantine zone the infected files. When the virus is in quarantine it can't do any harm.

The next step is selecting the report options. To do this you'll have to click the "+" sign corresponding to **Report options**. These options allow the creation of a report file (file that contains information about the scanning process).

Option		Description
Show all scanned files		Lists all scanned files and their status (infected or not) in a report file. With this option on, the computer will slow down.
Create report file	Report file name `<vscan.log>`	This is an edit field that allows changing the name of the report file. To do this, you'll have to simply click this option and type in a new name.
	Append to existing report	Select this option to append the information about the new scan process to the ones already existing in the report file.
	Limit report size to [1024] KB	Click this option and type the maximum file size in the edit field that appears.

In the **Performance options** category you can decrease the priority of the scan process. If you select the check box corresponding to **Run the task with Low priority** you will allow other programs to run faster and increase the time needed for the scan process to finish.

TIP: You can view the report file in the Report section from the **Antivirus** module.

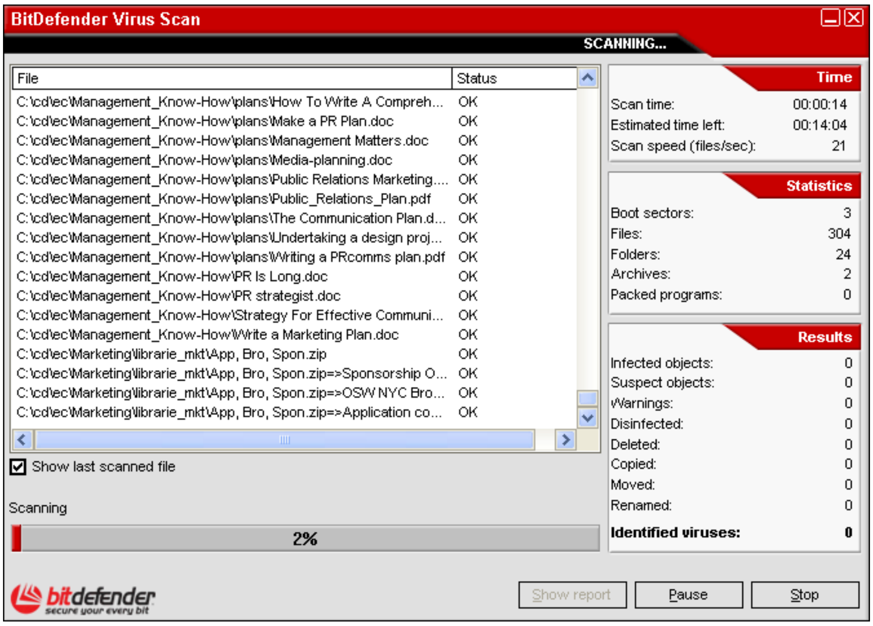
Note

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.

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

5. Scan for viruses

With the scan options selected, all you have to do is to effectively start the system scanning. For that, just click **Scan**. This may take a while, depending on the size of your hard disk drive!



File	Status
C:\cd\ec\Management_Know-How\plans\How To Write A Compreh...	OK
C:\cd\ec\Management_Know-How\plans\Make a PR Plan.doc	OK
C:\cd\ec\Management_Know-How\plans\Management Matters.doc	OK
C:\cd\ec\Management_Know-How\plans\Media-planning.doc	OK
C:\cd\ec\Management_Know-How\plans\Public Relations Marketing....	OK
C:\cd\ec\Management_Know-How\plans\Public_Relations_Plan.pdf	OK
C:\cd\ec\Management_Know-How\plans\The Communication Plan.d...	OK
C:\cd\ec\Management_Know-How\plans\Undertaking a design proj...	OK
C:\cd\ec\Management_Know-How\plans\Writing a PRcomms plan.pdf	OK
C:\cd\ec\Management_Know-How\PR Is Long.doc	OK
C:\cd\ec\Management_Know-How\PR strategist.doc	OK
C:\cd\ec\Management_Know-How\Strategy For Effective Communi...	OK
C:\cd\ec\Management_Know-How\Write a Marketing Plan.doc	OK
C:\cd\ec\Marketing\librarie_mkt\App, Bro, Spon.zip	OK
C:\cd\ec\Marketing\librarie_mkt\App, Bro, Spon.zip=>Sponsorship O...	OK
C:\cd\ec\Marketing\librarie_mkt\App, Bro, Spon.zip=>OSW NYC Bro...	OK
C:\cd\ec\Marketing\librarie_mkt\App, Bro, Spon.zip=>Application co...	OK

☑ Show last scanned file

Scanning

2%

Time	
Scan time:	00:00:14
Estimated time left:	00:14:04
Scan speed (files/sec):	21

Statistics	
Boot sectors:	3
Files:	304
Folders:	24
Archives:	2
Packed programs:	0

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

Figure 20

While scanning, BitDefender will show you its progress and alert you if any viruses are found.

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

If you click:

- **Stop** - a new window will appear where you can end the system verification. If you choose to end it, the **Stop** button will turn into a **Close** button and clicking it will close the scan window.
- **Pause** - the scan temporally stops - you can continue it by pressing **Resume**.
- **Show report** - the scan report will open.

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

TIP: In order to see the scanned files you must select **Show all scanned files** option from the report options (previous step). With this option on, the computer will slow down.

6. Alternative scanning methods

BitDefender has two alternative methods for scanning files immediately: using the contextual menu and by drag & drop feature.

Contextual scanning

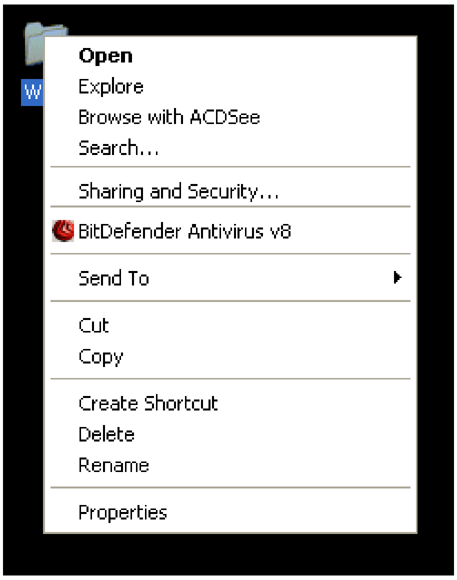


Figure 21

Right click the file or folder you want scanned and select the **Scan with BitDefender 8** option.

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

Drag & Drop scanning

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

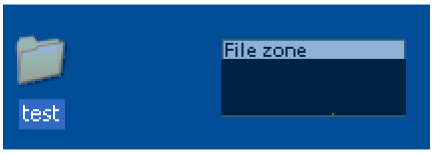


Figure 22

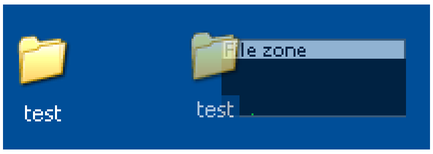
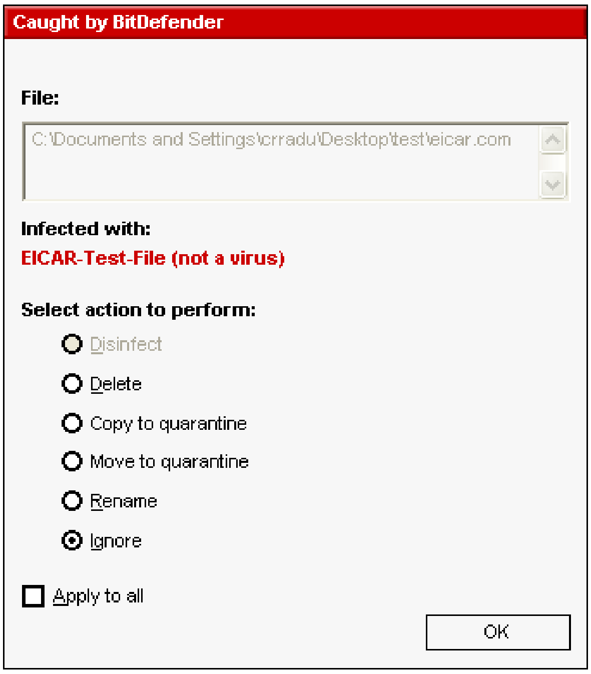


Figure 23

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

In both cases the scan window (Figure 20) will appear.

If a virus is detected, an alert window (Figure 24) will prompt you to select the action on the infected file.



Caught by BitDefender

File:

C:\Documents and Settings\crradu\Desktop\test\eicar.com

Infected with:

EICAR-Test-File (not a virus)

Select action to perform:

○ Disinfect

○ Delete

○ Copy to quarantine

○ Move to quarantine

○ Rename

● Ignore

□ Apply to all

Figure 24

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

You can select one of the following actions on the infected file:

- **Disinfect** - to disinfect the infected file.
- **Delete** – to delete the infected file.
- **Copy to quarantine** – to copy the infected file in the quarantine zone.
- **Move to quarantine** – to move the infected file to the quarantine zone.
- **Rename** – to change the extension of the infected files. The new extension of the infected files will be `.vir`.
- **Ignore** – to ignore the infection. No action will be taken on the infected file.

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

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

Finally, click **OK**.

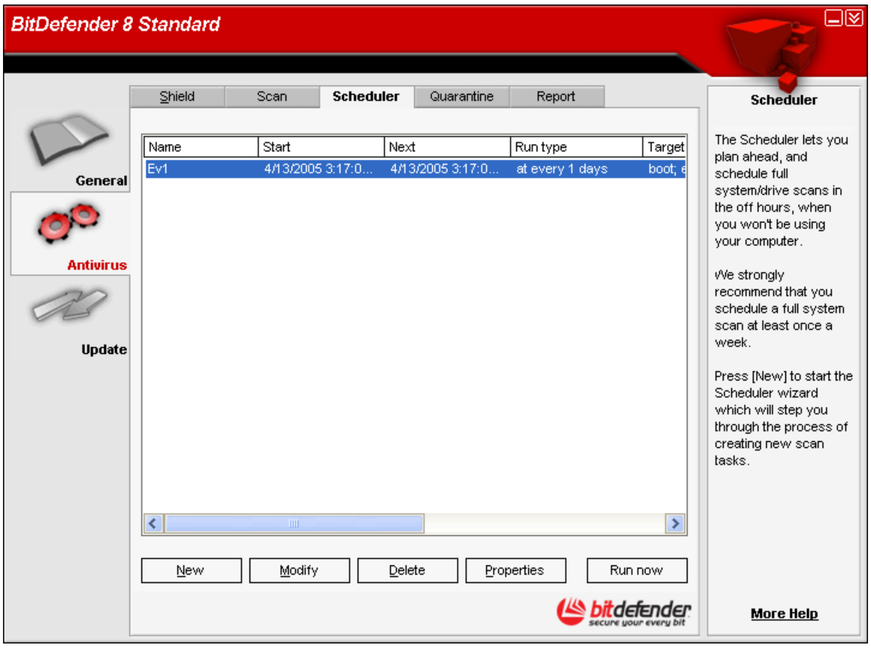
Scheduled scanning

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

It has the following features:

- A wizard for assistance in creating scheduled scan tasks;
- Scan frequency selection;
- Drives and/or folders selection;
- File extensions selection;
- Distinct configuration module for each scan job;
- LAN scanning facilities;
- Automatic isolation of the infected or suspicious files in the quarantine zone;
- Background scanning, with no interference with the user's activity;
- Scheduled task properties summary;
- Generates scanning reports.

In the management console, enter the **Antivirus** module and click the **Scheduler** tab.



Name	Start	Next	Run type	Target
Ev1	4/13/2005 3:17:0...	4/13/2005 3:17:0...	at every 1 days	boot;

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

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

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

Figure 25

The **Scheduler** section contains a few buttons for administrating the scan tasks:

➔ **New** – launches the wizard that will guide you through the creation of a new scan task.

➔ **Modify** – modifies the properties of a previously created task. It also launches the wizard.

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

➔ **Delete** – deletes a selected task.

➔ **Properties** – views the properties of the selected task.

➔ **Run now** – starts immediately the selected task.

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

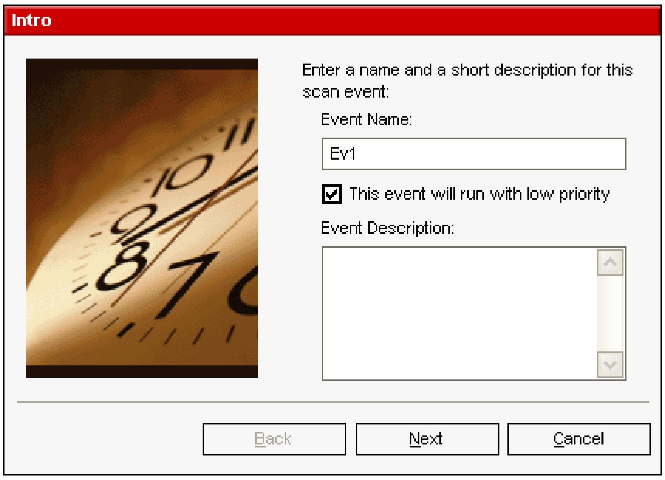
The **Scheduler** includes a wizard for creating new scan tasks. This will assist you any time you need to do any operation with these scan events, no matter if it's creating a new task or modifying an existing one.

Click **New**. This will launch the scan task creation wizard.

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

1. Intro

The first move is to specify a name for the new task.



Intro

Enter a name and a short description for this scan event:

Event Name: Ev1

☑ This event will run with low priority

Event Description:

Figure 26

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

Click **Next** to continue.

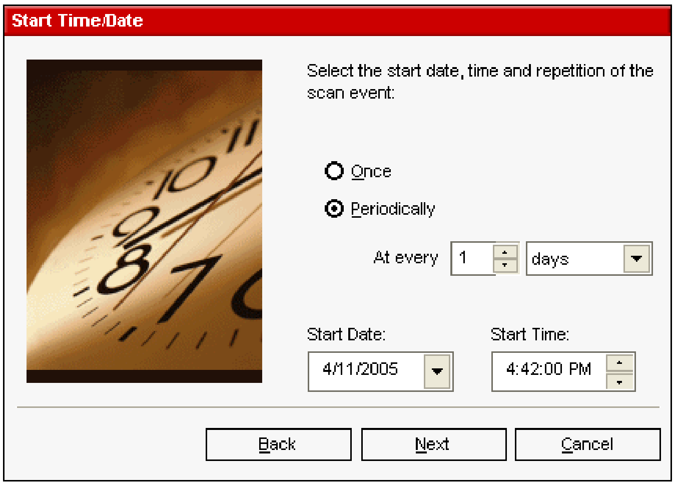
Select the check box corresponding to **This event will run with low priority** if you want to decrease the priority of the scan task and allow other programs to run faster. This will increase the time needed for the task to finish.

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

2. Start Time/Date

Further on, a window where you can select the scan type will appear.

Select the check box corresponding to **Once** if you want to schedule a one time scan. If you want the scan to be repeated after certain intervals, select the check box corresponding to **Periodically**.



Start Time/Date

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

○ Once

● Periodically

At every 1 days

Start Date: 4/11/2005

Start Time: 4:42:00 PM

Figure 27

Type in the **At every** edit box the number of minutes / hours / days / weeks / months / years you want to repeat this process.

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

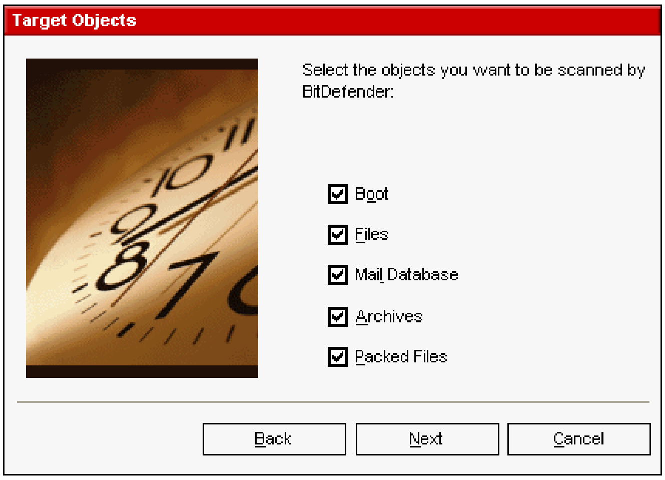
Select the interval - minutes, hours, days, weeks, months, years - to which the scan be repeated. Scroll down the list and click the time unit you want.

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

After selecting the period, click **Next** to continue. If you wish to go back to the previous step, click **Back**.

3. Target Objects

This step is to select the objects you want to be scanned - the boot sector, the files, the archives and the packed files.



Target Objects

Select the objects you want to be scanned by BitDefender:

☑ Boot

☑ Files

☑ Mail Database

☑ Archives

☑ Packed Files

Figure 28

Select one or more objects to scan, by simply checking each one you want.

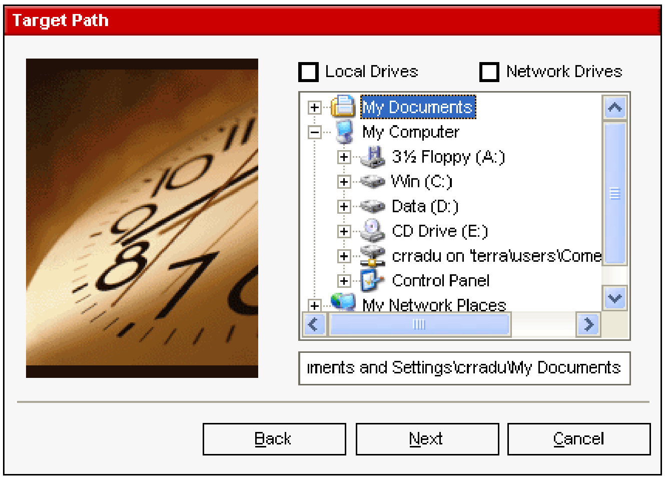
You can select one of the following objects:

- **Boot** – to scan the boot sector, in order to identify the boot viruses;
- **Files** – to scan files;
- **Mail database** – to scan mail archives in order to detect mail viruses;
- **Archives** – to scan inside archives;
- **Packed files** – to scan packed files.

Click **Next**.

4. Target Path

Here you have to specify the path to the objects that will be scanned, as observed in the picture. This step is necessary if you have selected to scan files in the previous step.



iments and Settings\crradu\My Documents

Figure 29

This screen is actually an exploring window that lets you select the partitions and folders to be scanned.

When the cursor is placed on a folder, the complete path to the folder will appear in the field placed under this exploring window.

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

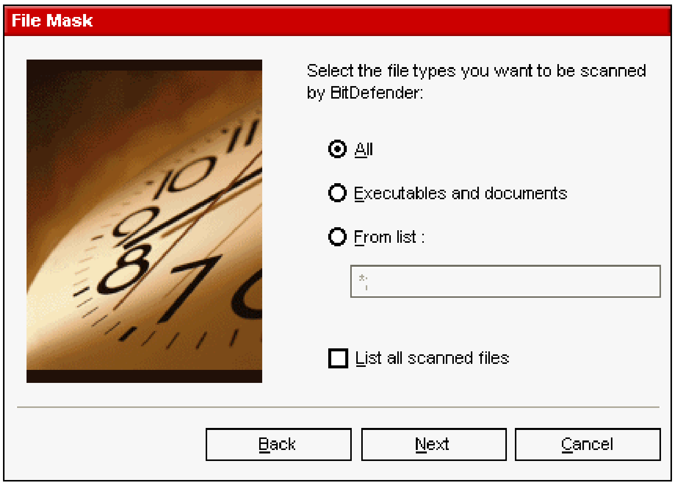
Also, in order to select the locations to be scanned, you can use the fast-selection options placed on the topside of the window:

- ➔ **Local Drives** – to scan all local drives;
- ➔ **Network Drives** – to scan all network drives.

Click **Next**.

5. File Mask

Specify the types of the files that will be scanned.



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

- ● All
- ○ Executables and documents
- ○ From list :

*;

□ List all scanned files

Figure 30

This step is needed only in case you choose to scan files.

You can select:

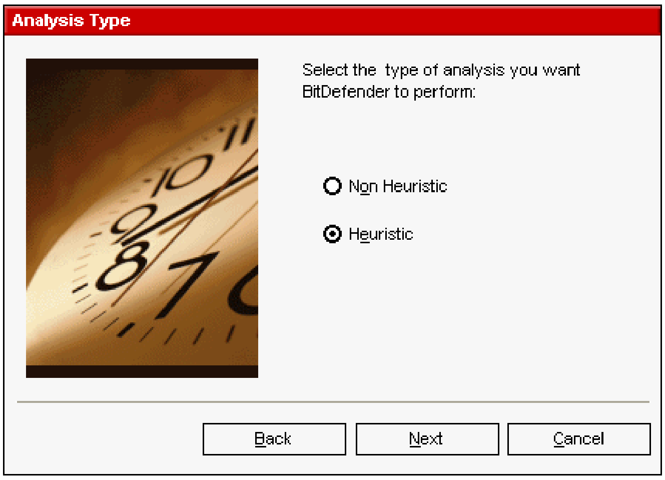
- ➔ **All** – to scan all files, no matter what their type is;
- ➔ **Executables and documents** – to scan the program files and documents;
- ➔ **From list** – to scan only the files whose extensions appear in the list. These extensions must be separated by a semicolon “;”.

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

Click **Next**.

6. Analysis Type

Select the scan type.



Analysis Type

Select the type of analysis you want BitDefender to perform:

○ Non Heuristic

● Heuristic

Figure 31

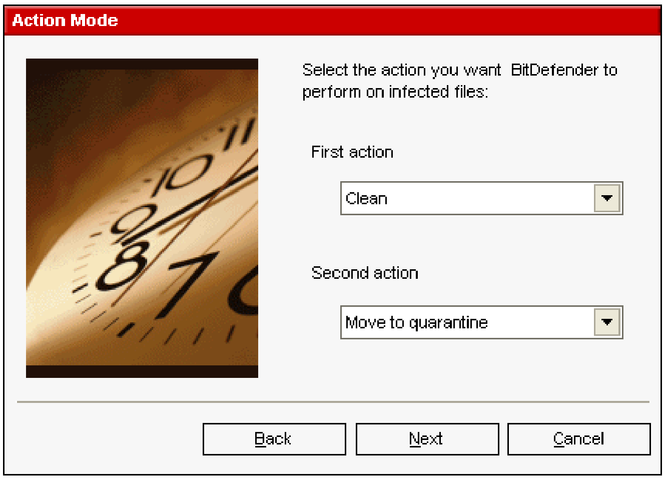
This, as it can be observed from the picture, implies selecting one of the two scan types:

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

Click **Next**.

7. Action mode

BitDefender allows selecting two actions in case an infected file is found.



Action Mode

Select the action you want BitDefender to perform on infected files:

First action: Clean

Second action: Move to quarantine

Figure 32

You can select the first and the second action.

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

For the first action the following options are available:

First Action	Description
Clean file	To disinfect the infected files.
Delete file	To automatically delete, without any warning, all the infected files. Action not recommended!
Move to quarantine	To move the infected files from the initial location to the quarantine zone. When the virus is in quarantine it can't do any harm.
Rename	To change the extension of the infected files. The new extension of the infected files will be `.vir`. By renaming the infected files, the possibility of executing and thus of spreading the infection is removed. At the same time they can be saved for further examination and analysis.
Prompt	Every time an infected file is detected, a dialog box is shown, where the user can select the action to perform on that file. It is recommended that you select an action depending on the importance of that file.
Ignore	In this case the infection is ignored and no action will be taken on the infected file. Only its status will be reported.

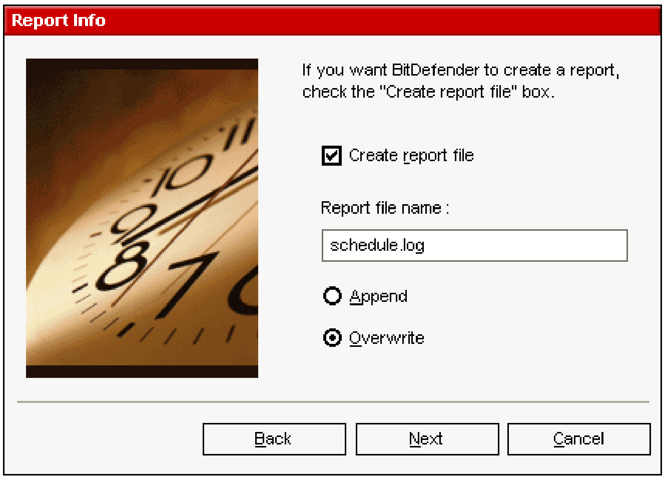
For the second action the following options are available:

Second Action	Description
Delete file	To automatically delete, without any warning, all the infected files.
Move to quarantine	To move the infected files from the initial location to the quarantine zone. When the virus is in quarantine it can't do any harm.
Rename	To change the extension of the infected files. The new extension of the infected files will be `.vir`. By renaming the infected files, the possibility of executing and thus of spreading the infection is removed. At the same time they can be saved for further examination and analysis.
Prompt	Every time an infected file is detected, a dialog box is shown, where the user can select the action to perform on that file. It is recommended that you select an action depending on the importance of that file.
Ignore	In this case the infection is ignored and no action will be taken on the infected file. Only its status will be reported.

Click **Next**.

8. Report Info

Choose how to create a scan report file.



Report Info

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

☑ Create report file

Report file name : schedule.log

○ Append

● Overwrite

Figure 33

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

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

Click **Append** in case you want to append to an existing report file the information about the new scanning, building this way a small historical of the scan results performed at different moments.

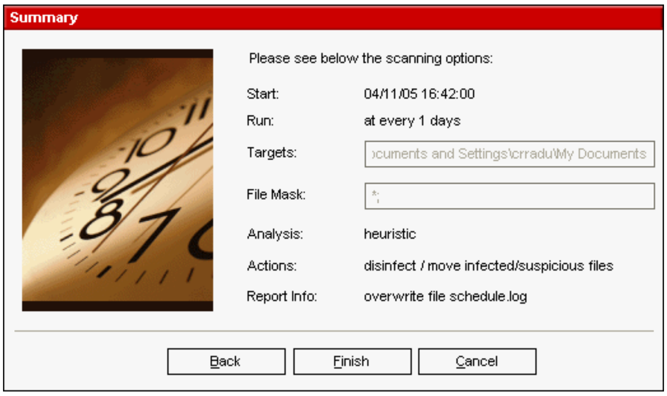
Click **Overwrite** if you wish to create a new report file every time a new scan is launched. In this case the information about the previous scanning will be deleted.

Tip: You can view the report file in the Report section from the Antivirus module.

Click **Next**.

9. Summary

This is the last step in the creation of a scan event.



Summary

Please see below the scanning options:

Start: 04/11/05 16:42:00

Run: at every 1 days

Targets: ›cuments and Settings\crradu\My Documents

File Mask: *;

Analysis: heuristic

Actions: disinfect / move infected/suspicious files

Report Info: overwrite file schedule.log

Figure 34

In this window you can view all the settings for the scan event and you can make any changes, by returning to the previous steps (**Back**). If you do not want to make any modifications, click **Finish**.

The new event will appear in the **Scheduler** section.

For each scheduled scan event, you can view its name, its description, the starting date, the next moment when it will be launched, the scan type (periodically or one time scan), the target, the files extensions, the analysis type and the action on the infected files.

Note

When modifying a scan event, the same steps will be followed. In case the name of the event modifies, a new event will be created. For example, if we have the event EV1 and have modified its name into EV2, EV1 will not disappear, on the contrary, a new event named EV2, having the same properties as EV1, will appear.

If you right click a scheduled event, a pop menu, like the one you see in the picture below will appear:

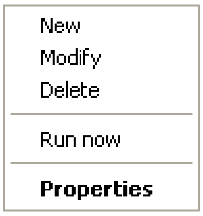


Figure 35

If no event is selected, and you right click the **Scheduler** section, only **New** option will be enabled, all others being disabled.

TIP: The Scheduler allows an unlimited number of scheduled scan events.

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

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

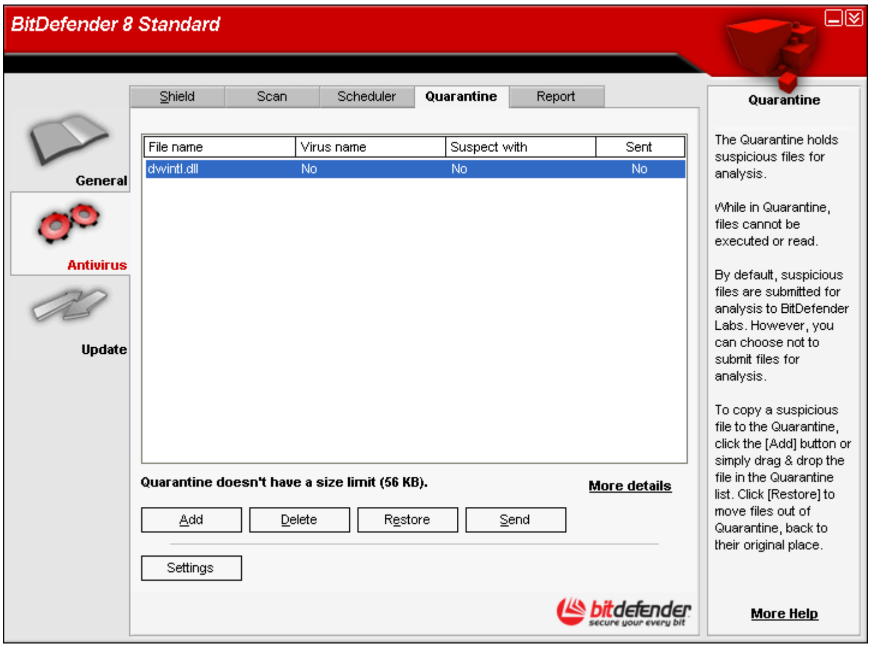
Isolating the infected files

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

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

In case you haven't already opened the management console, you can access it from the Windows Start menu, following the path **Start** → **Programs** → **BitDefender** → **BitDefender 8 Standard** or quicker, double click the BitDefender icon from the system tray.

In the management console, enter the **Antivirus** module and click the **Quarantine** tab.



File name	Virus name	Suspect with	Sent
dwintl.dll	No	No	No

Quarantine doesn't have a size limit (56 KB).

Quarantine

The Quarantine holds suspicious files for analysis.

While in Quarantine, files cannot be executed or read.

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

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

Figure 36

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

Note

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

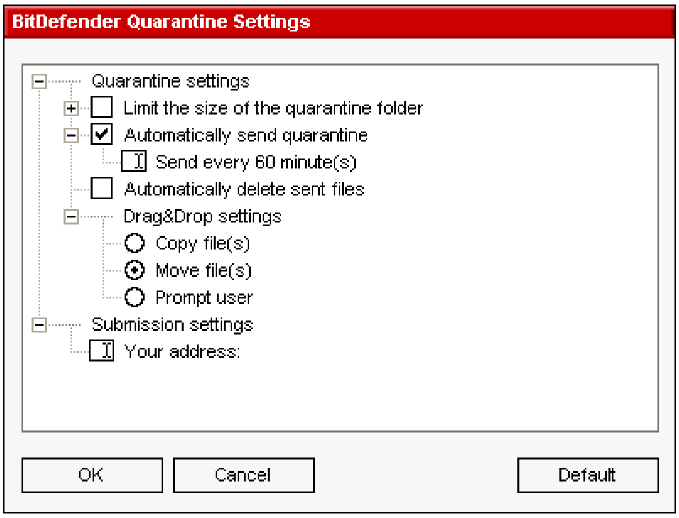
The **Quarantine** section contains a few buttons for administrating these files:

- **Add** – ads files to quarantine. Use this button to quarantine a file you suspect of being infected. A window will open and you can select the file from its location on the disk. This way the file is copied to quarantine. If you want to move the file in the quarantine zone you must select the checkbox corresponding to **Delete from original location**. A quicker method to add suspicious files to the Quarantine is to drag & drop them in the quarantine list.

- **Delete** – deletes the selected file from your computer.
- **Restore** – returns the selected file to its original location.
- **Send** – sends the selected files for further analysis to the BitDefender lab. You must specify some information before you may submit these files. For that click **Settings** and complete the fields from the **E-mail settings** section, as described below.

> **Note**
>
> By default, suspicious files are submitted for analysis to the BitDefender Labs. However, you can choose not to submit files for analysis by deselecting the **Automatically send quarantine** option from the Quarantine settings.

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



BitDefender Quarantine Settings

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

Figure 37

The quarantine options are grouped in two categories:

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

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

Quarantine settings

- **Limit the size of the quarantine folder** - maintains under control the size of the quarantine. This option is enabled by default and its size is 12000 KB. If you want to change this value you can introduce it in **The maximum size of the quarantine folder is** field.

  The **Automatically delete old files** option is used to delete old files when the quarantine is full and there is no space to add new files.

- **Automatically send quarantine** – sends automatically the quarantined files to the BitDefender Labs for further analysis. You can set the time period between two consecutive sending processes in minutes in the **Send quarantine every** field.
- **Automatically delete sent files** – deletes automatically the quarantined files after sending them to the BitDefender Lab for analysis.
- **Drag & Drop settings** – if you are using the Drag & Drop method to add files to the quarantine here you can specify the action: copy, move or prompt user.

Submission settings

You must specify your e-mail address in order to send the quarantined files to the BitDefender Labs.

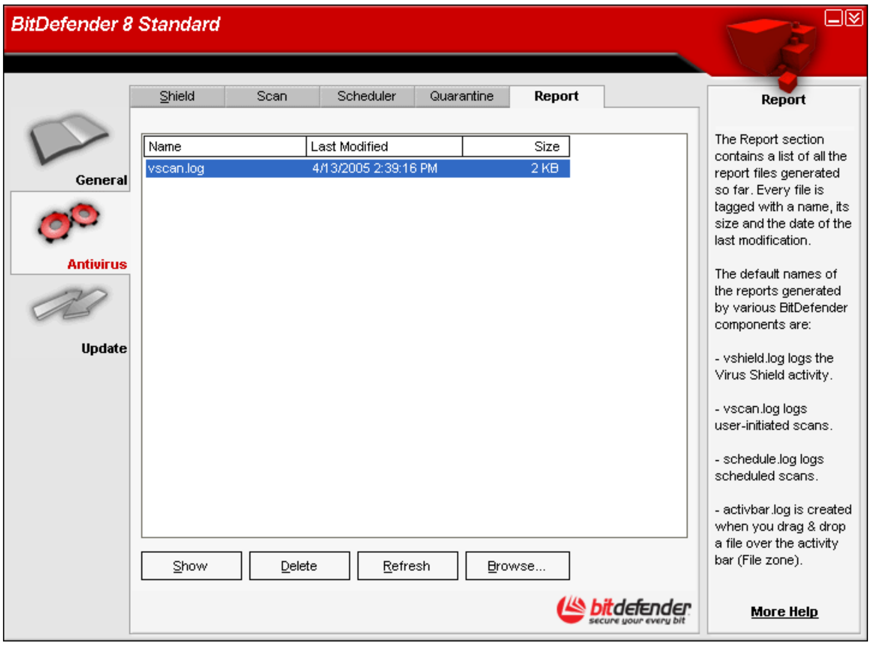
- **Your address** – enter your e-mail address in case you want to receive e-mail from our experts, regarding the suspicious files submitted for analysis.

Viewing the report files

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

In case you haven't already opened the management console, you can access it from the Windows Start menu, following the path **Start** → **Programs** → **BitDefender** → **BitDefender 8 Standard** or quicker, double click the BitDefender icon from the system tray.

In the management console, enter the **Antivirus** module and click the **Report** tab.



Name	Last Modified	Size
vscan.log	4/13/2005 2:39:16 PM	2 KB

Report

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

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

- vshield.log logs the Virus Shield activity.

- vscan.log logs user-initiated scans.

- schedule.log logs scheduled scans.

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

Figure 38

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

- Vshield.log is the log BitDefender writes to when it continuously scans and protects your e-mail messages, downloads and active programs or files on your system;
- Vscan.log is created when you scan your system immediately;
- Schedule.log is from the scheduled scans you may have set up;
- Activbar.log is created when you scan by drag & drop feature.

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

There are some buttons created for the administration of these report files. The function of each button is explained further:

➔ **Show** – opens the selected report file.
➔ **Delete** – deletes the selected file report.

- **Refresh** – if the management console is open at the **Report** section and in the meantime you perform a scan of your computer, the new report file with the scan results (if you selected the **Create report file** option) will be visible only after you click **Refresh**.
- **Browse** – opens a window in which you can select the report files you want to see.

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

Removing a found virus

Viruses are much easier to stop from entering your system, rather than removing them once they are inside your computer. This is why the virus protection should always be enabled and updated.

If BitDefender does detect a resident virus it is recommended to let BitDefender try to remove it. This may fail for various reasons - resident viruses, already active on your system may be very tricky to deal with.

If BitDefender finds a virus and it is not able to clean your system it is recommended that you contact our support team at support@bitdefender.com.

The secret to removing a virus successfully is to know all about it. You can find additional virus-info on our website, www.bitdefender.com.

For the most wide-spread viruses we offer special removal tool.

It is always a good idea to search the Internet for all the information you can find about the virus in question.

Contact our free support at support@bitdefender.com for more help.

Update module

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

Features

Updates come in three flavors:

- **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**;
- **Updates for antivirus engines** - as new threats appear, the files containing virus signatures must be updated to ensure permanent up-to-date protection against them. This goes under the name of **Virus Definitions Update**.

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

- **Manual update** – verifying the existence of an update by user request;
- **Automatic update** – the antivirus automatically contacts the BitDefender server in order to check if an update was released. If so, BitDefender is updated automatically.

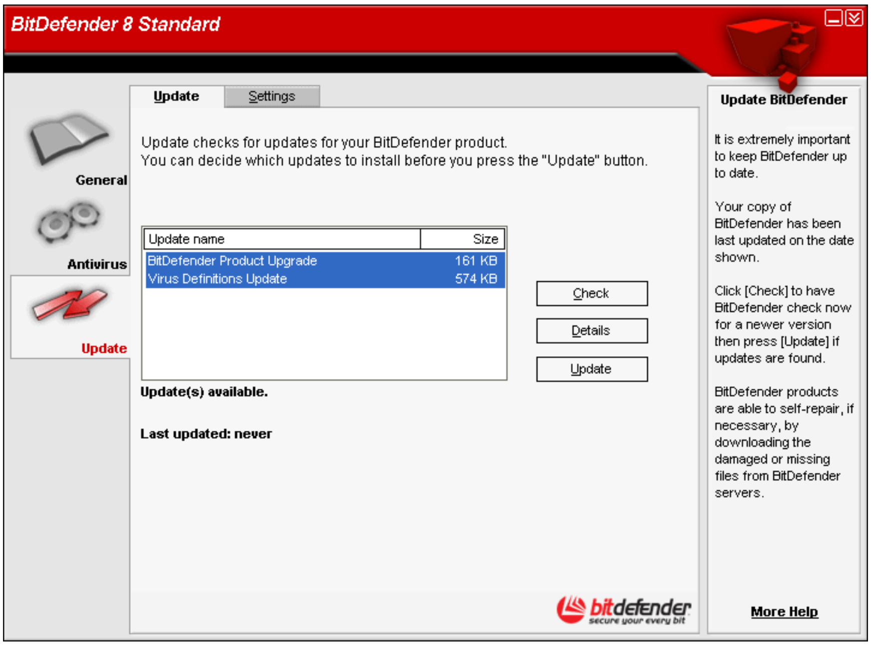
If you are connected to the Internet through broadband or DSL, BitDefender takes care of this itself: It checks for new virus signatures when you turn on your computer and every **3 hours** after that. If any new virus signatures are available, BitDefender will update itself.

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

Manual update

In case you haven't already opened the management console, you can access it from the Windows Start menu, following the path **Start** → **Programs** → **BitDefender** → **BitDefender 8 Standard** or quicker, double click the BitDefender icon from the system tray.

In the management console, click **Update**.



Update checks for updates for your BitDefender product.
You can decide which updates to install before you press the "Update" button.

Update name	Size
BitDefender Product Upgrade	161 KB
Virus Definitions Update	574 KB

Update(s) available.

Last updated: never

Update BitDefender

It is extremely important to keep BitDefender up to date.

Your copy of BitDefender has been last updated on the date shown.

Click [Check] to have BitDefender check now for a newer version then press [Update] if updates are found.

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

Figure 39

The manual update can be done anytime, even when the product was set on automatic update. To manually update the product you must follow the steps:

- Click **Check**. The **Update** module will connect to the BitDefender update server and will verify if any update is available.
- If an update was detected, its name and size will be displayed. Click **Update** to start the update process.

TIP: If you want to see which files will be updated, click **Details**.

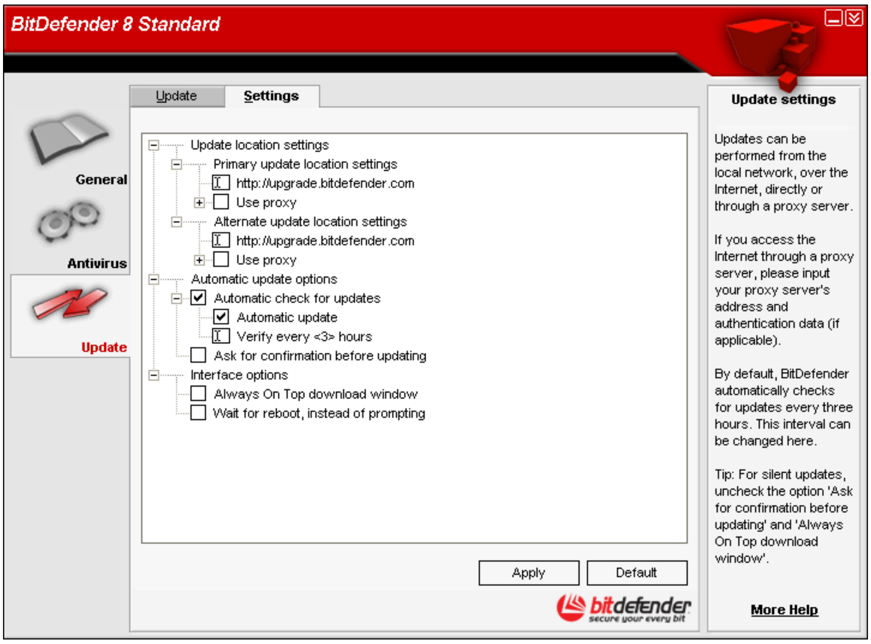
If there is no update available a message will appear.

Note

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

Automatic update

If you're an advanced user, click the **Settings** tab in order to configure the **Update** module.



```
⊟ Update location settings
   ⊟ Primary update location settings
        http://upgrade.bitdefender.com
      ⊞ □ Use proxy
   ⊟ Alternate update location settings
        http://upgrade.bitdefender.com
      ⊞ □ Use proxy
⊟ Automatic update options
   ⊟ ☑ Automatic check for updates
        ☑ Automatic update
        Verify every <3> hours
     □ Ask for confirmation before updating
⊟ Interface options
     □ Always On Top download window
     □ Wait for reboot, instead of prompting
```

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

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

By default, BitDefender automatically checks for updates every three hours. This interval can be changed here.

Tip: For silent updates, uncheck the option 'Ask for confirmation before updating' and 'Always On Top download window'.

Figure 40

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

The window with the update settings contains three categories of options (**Update location settings**, **Automatic update options**, **Interface options**) organized in an expandable menu, similar to the ones from Windows.

Click the box labeled "+" to open an option or click the one labeled "-" to close an option.

Update location settings

For more reliable and faster updates, you can configure two update locations: a **Primary update location** and an **Alternate update location**. For both of them you must configure the following options:

➔ If you are connected to a local network that has BitDefender virus signatures placed locally, you can change the location of the updates here. By default this is: http://upgrade.bitdefender.com.

➔ **Use proxy** - In case the company uses a proxy server check this option. The following settings must be specified.

- **Proxy sets** - type in the IP or the name of the proxy server and the port BitDefender uses to connect to the proxy server.

  ! Syntax: `name:port` or `ip:port`.

- **Proxy user -** type in a user name recognized by the proxy.

Syntax: `domain\user`.

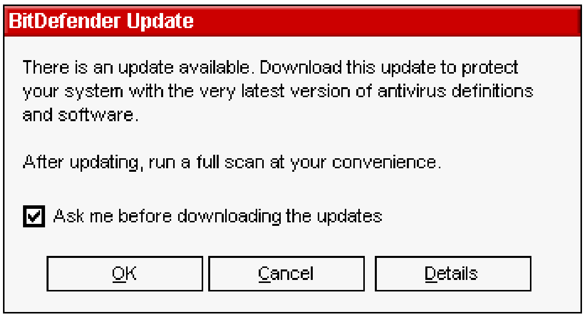
- **Proxy password -** type in the valid password for the previously specified user

Automatic update options

➔ **Automatic check for updates** – This ensures that BitDefender automatically checks our servers for available updates.

- **Automatic update** - If BitDefender detects a new update on our servers, then with this option on, BitDefender downloads and implements the update.
- **Verify every <x> hours** - Sets how often BitDefender checks for updates The default time interval is 3 hours.

➔ Keep selected **Ask for confirmation before updating** in order to be asked before downloading and installing the updates.



BitDefender Update

There is an update available. Download this update to protect your system with the very latest version of antivirus definitions and software.

After updating, run a full scan at your convenience.

☑ Ask me before downloading the updates

Figure 41

Click **OK** to start the update process or click **Cancel** to update later.

If you click **Details** you will see which files will be updated.

Interface options

➔ **Always On Top download window** - By default the product update is done in the background. If you wish the update to be made in foreground, meaning that a window reflecting the update stage will appear above all other windows, use this option.

➔ **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.

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

6

Best practices

Antivirus

Steps to follow in order to ensure a computer free from viruses:

1. After the installation process is over, please register your product, as described in the Product registration section.
2. Perform a manual update of your virus signatures. In the **BitDefender Management Console**, enter the **Update** module and click **Check**.
3. Perform a full scan of your system (described in the Immediate scanning section of this user guide).
4. In the Status section of the **General** module, keep enabled the most important antivirus features of BitDefender: Virus Shield and Automatic update.
5. Program your BitDefender to scan your system at least once a week, using the Scheduler wizard.

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

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

7

Frequently Asked Questions

General

1. **Q:** How can I tell if BitDefender is actually working?
   A: In the **General** module, access the Status section and look at the statistics.

2. **Q:** What are the system requirements?
   A: You can see the system requirements in the Installation section.

3. **Q:** How do I uninstall BitDefender?
   A: Follow the path: **Start** → **Programs** → **BitDefender 8** → **Modify, Repair or Uninstall** and in the window that will appear click the **Remove** button. This will start the uninstall process.

4. **Q:** Where do I enter my serial number (license key)?
   A: In the **General** module, access the Registration section and click the **Enter new key** button.

Antivirus

5. **Q:** How can I perform a full system scan?
   A: In the **General** module, access the Scan section, check **Local drives** and click **Scan**.

6. **Q:** How often should I scan my computer?
   A: We recommend you to scan your computer at least once a week.

7. **Q:** How can I automatically scan every file that I transfer to my computer?
   A: BitDefender scans all files on-access. All you have to do is to keep Virus Shield enabled.

8. **Q:** How can I program BitDefender to scan my computer periodically?
   A: In the **General** module, access the Scheduler section, click **New** and follow the wizard.

9. **Q:** What happens with the files from the quarantine zone?
   A: You can send these files to the BitDefender Labs in order to be analyzed, but first you must specify the e-mail settings (access the Quarantine section and click **Settings**).

Update

10. **Q:** Why is it necessary to update BitDefender?
A: Every time you perform an update new virus signatures will be added to the scan engines, new rules will be added to the Heuristic & URL filters.

11. **Q:** How can I update BitDefender?
A: By default, BitDefender will automatically update every 3 hours. But you can also update manually or change the time interval for the automatic update in the Update module.

8

Vocabulary

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.

Archive

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

(2) 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.
The Scheduler is a tool that helps you schedule scan events.

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

1.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, stating the drive, directory, any subdirectories, the file itself, and its filename extension if it has one: `c:jobscompany/resume.txt`. This complete set of information is a fully qualified path.

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

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

(1) 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.

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

Report file

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

Script

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

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.

Contact information

As a valued provider, SOFTWIN strives to provide its customers an unparallel level of fast and accurate support. The Support Center is continually updated with the newest virus descriptions and answers to common questions to help you find answers to your problems in a timely manner.

We at SOFTWIN, are dedicated to saving customer's time and money by providing the most advanced products at the fairest prices. We think that a successful business has a lot to do with good communication and a commitment to excellence in customer support.

Sales department: sales@bitdefender.com

http://buy.bitdefender.com

Technical support: support@bitdefender.com

Phone: 0040-21-233 07 80

Product web site: www.bitdefender.com

Find a local distributor: www.bitdefender.com/partner_list/

Address:
SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest, ROMANIA