

ANTIVIRUS  
PLUS 2012

**Bitdefender**®



User's Guide

# Bitdefender Antivirus Plus 2012

## Bitdefender Antivirus Plus 2012 *User's Guide*

Publication date 2011.07.27

Copyright© 2011 Bitdefender

### Legal Notice

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

**Warning and Disclaimer.** This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of Bitdefender, therefore Bitdefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. Bitdefender provides these links only as a convenience, and the inclusion of the link does not imply that Bitdefender endorses or accepts any responsibility for the content of the third-party site.

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



## Table of Contents

1. Installation .....	1
1.1. Preparing for installation .....	1
1.2. System requirements .....	1
1.2.1. Minimum system requirements .....	1
1.2.2. Recommended system requirements .....	2
1.2.3. Software requirements .....	2
1.3. Installing your Bitdefender product .....	2
1.3.1. Upgrading from an older version .....	5
2. Getting started .....	6
2.1. Opening Bitdefender .....	6
2.2. What you have to do after installation .....	6
2.3. Product registration .....	7
2.3.1. Entering your license key .....	7
2.3.2. Logging in to MyBitdefender .....	8
2.3.3. Buying or renewing license keys .....	10
2.4. Fixing issues .....	10
2.4.1. Fix All Issues wizard .....	10
2.4.2. Configuring status alerts .....	11
2.5. Events .....	12
2.6. Auto Pilot .....	12
2.7. Game Mode and Laptop Mode .....	13
2.7.1. Game Mode .....	13
2.7.2. Laptop Mode .....	15
2.8. Password-protecting Bitdefender settings .....	15
2.9. Anonymous usage reports .....	16
2.10. Repairing or removing Bitdefender .....	16
3. Bitdefender interface .....	18
3.1. System tray icon .....	18
3.2. Main window .....	19
3.2.1. Upper toolbar .....	20
3.2.2. Panels area .....	20
3.3. Settings window .....	22
4. How to .....	24
4.1. How do I register a trial version? .....	24
4.2. How do I register Bitdefender without an Internet connection? .....	25
4.3. How do I upgrade to another Bitdefender 2012 product? .....	26
4.4. When should I reinstall Bitdefender? .....	26
4.5. When does my Bitdefender protection expire? .....	26
4.6. How do I renew my Bitdefender protection? .....	27
4.7. What Bitdefender product am I using? .....	27
4.8. How do I scan a file or a folder? .....	28
4.9. How do I scan my system? .....	28
4.10. How do I create a custom scan task? .....	28
4.11. How do I exclude a folder from being scanned? .....	28
4.12. What to do when Bitdefender detected a clean file as infected? .....	29

4.13. How do I protect my personal information? .....	30
4.14. How do I configure Bitdefender to use a proxy Internet connection? .....	30
<b>5. Antivirus protection .....</b>	<b>32</b>
5.1. On-access scanning (real-time protection) .....	33
5.1.1. Checking malware detected by on-access scanning .....	33
5.1.2. Adjusting the real-time protection level .....	33
5.1.3. Creating a custom protection level .....	34
5.1.4. Restoring the default settings .....	35
5.1.5. Turning on or off real-time protection .....	36
5.1.6. Actions taken on detected malware .....	36
5.2. On-demand scanning .....	37
5.2.1. Auto Scan .....	37
5.2.2. Scanning a file or folder for malware .....	38
5.2.3. Running a Quick Scan .....	38
5.2.4. Running a Full System Scan .....	38
5.2.5. Configuring and running a custom scan .....	39
5.2.6. Antivirus Scan Wizard .....	41
5.2.7. Checking scan logs .....	44
5.3. Automatic scan of removable media .....	44
5.3.1. How does it work? .....	44
5.3.2. Managing removable media scan .....	45
5.4. Configuring scan exclusions .....	46
5.4.1. Excluding files or folders from scanning .....	46
5.4.2. Excluding file extensions from scanning .....	47
5.4.3. Managing scan exclusions .....	47
5.5. Managing quarantined files .....	48
5.6. Active Virus Control .....	49
5.6.1. Checking detected applications .....	49
5.6.2. Turning on or off Active Virus Control .....	49
5.6.3. Adjusting the Active Virus Control protection .....	50
5.6.4. Managing excluded processes .....	50
5.7. Fixing system vulnerabilities .....	51
5.7.1. Scanning your system for vulnerabilities .....	51
5.7.2. Using automatic vulnerability monitoring .....	52
<b>6. Privacy Control .....</b>	<b>55</b>
6.1. Antiphishing protection .....	55
6.1.1. Bitdefender protection in the web browser .....	56
6.1.2. Bitdefender alerts in the browser .....	57
6.2. Data Protection .....	58
6.2.1. About data protection .....	58
6.2.2. Configuring data protection .....	58
6.2.3. Managing Rules .....	60
6.3. Chat Encryption .....	60
<b>7. Network Map .....</b>	<b>62</b>
7.1. Enabling the Bitdefender network .....	62
7.2. Adding computers to the Bitdefender network .....	63
7.3. Managing the Bitdefender network .....	63

8. Update .....	66
8.1. Checking if Bitdefender is up-to-date .....	66
8.2. Performing an update .....	67
8.3. Turning on or off automatic update .....	67
8.4. Adjusting update settings .....	67
9. Safego protection for social networks .....	70
10. Troubleshooting .....	71
10.1. My system appears to be slow .....	71
10.2. Scan doesn't start .....	72
10.3. I can no longer use an application .....	72
10.4. How to update Bitdefender on a slow Internet connection .....	73
10.5. My computer is not connected to the Internet. How do I update Bitdefender? ..	74
10.6. Bitdefender services are not responding .....	74
10.7. Bitdefender removal failed .....	75
10.8. My system doesn't boot up after installing Bitdefender .....	75
11. Removing malware from your system .....	77
11.1. Bitdefender Rescue Mode .....	77
11.2. What to do when Bitdefender finds viruses on your computer? .....	79
11.3. How do I clean a virus in an archive? .....	80
11.4. How do I clean a virus in an e-mail archive? .....	81
11.5. What to do if I suspect a file as being dangerous? .....	82
11.6. How to clean the infected files from System Volume Information .....	82
11.7. What are the password-protected files in the scan log? .....	83
11.8. What are the skipped items in the scan log? .....	84
11.9. What are the over-compressed files in the scan log? .....	84
11.10. Why did Bitdefender automatically delete an infected file? .....	84
12. Getting help .....	85
12.1. Support .....	85
12.1.1. Online resources .....	85
12.1.2. Asking for help .....	86
12.2. Contact information .....	88
12.2.1. Web addresses .....	88
12.2.2. Local distributors .....	88
12.2.3. Bitdefender offices .....	88
13. Useful information .....	91
13.1. How do I remove other security solutions? .....	91
13.2. How do I restart in Safe Mode? .....	92
13.3. Am I using a 32 bit or a 64 bit version of Windows? .....	92
13.4. How do I use System Restore in Windows? .....	93
13.5. How do I display hidden objects in Windows? .....	93
Glossary .....	94

## 1. Installation

### 1.1. Preparing for installation

Before you install Bitdefender Antivirus Plus 2012, complete these preparations to ensure the installation will go smoothly:

- Make sure that the computer where you plan to install Bitdefender meets the minimum system requirements. If the computer does not meet all the minimum system requirements, Bitdefender will not be installed or, if installed, it will not work properly and it will cause system slowdowns and instability. For a complete list of system requirements, please refer to *"System requirements"* (p. 1).
- Log on to the computer using an Administrator account.
- Remove any other similar software from the computer. Running two security programs simultaneously may affect their operation and cause major problems with the system. Windows Defender will be disabled during the installation.
- It is recommended that your computer be connected to the Internet during the installation, even when installing from a CD/DVD. If newer versions of the application files than those included in the installation package are available, Bitdefender will download and install them.

### 1.2. System requirements

You may install Bitdefender Antivirus Plus 2012 only on computers running the following operating systems:

- Windows XP with Service Pack 3 (32-bit)
- Windows Vista with Service Pack 2
- Windows 7 with Service Pack 1

Before installation, make sure that your computer meets the minimum system requirements.



#### Note

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

#### 1.2.1. Minimum system requirements

- 1.8 GB available free hard disk space (at least 800 MB on the system drive)
- 800 MHz processor
- 1 GB of memory (RAM)

## 1.2.2. Recommended system requirements

- 2.8 GB available free hard disk space (at least 800 MB on the system drive)
- Intel CORE Duo (1.66 GHz) or equivalent processor
- Memory (RAM):
  - ▶ 1 GB for Windows XP
  - ▶ 1.5 GB for Windows Vista and Windows 7

## 1.2.3. Software requirements

To be able to use Bitdefender and all its features, your computer needs to meet the following software requirements:

- Internet Explorer 7 or higher
- Mozilla Firefox 3.6 or higher
- Yahoo! Messenger 8.1 or higher
- .NET Framework 3

## 1.3. Installing your Bitdefender product

You can install Bitdefender from the Bitdefender installation disc or using a web installer downloaded on your computer from the Bitdefender website or from other authorized websites (for example, the website of a Bitdefender partner or an online shop). You can download the installation file from the Bitdefender website at the following address: <http://www.bitdefender.com/site/Downloads/>.

- To install Bitdefender from the installation disc, insert the disc in the optical drive. A welcome screen should be displayed in a few moments. Follow the instructions to start installation.



### Note

The welcome screen provides an option to copy the installation package from the installation disc to a USB storage device. This is useful if you need to install Bitdefender on a computer that does not have a disc drive (for example, on a netbook). Insert the storage device into the USB drive and then click **Copy to USB**. Afterwards, go to the computer without a disc drive, insert the storage device into the USB drive and double-click `runsetup.exe` from the folder where you have saved the installation package.

If the welcome screen does not appear, go to the disc's root directory and double-click the file `autorun.exe`.

- To install Bitdefender using the web installer downloaded on your computer, locate the file and double-click it. This will initiate the download of the installation files, which may take a while, depending on your Internet connection.

Bitdefender will first check your system to validate the installation.



If your system does not meet the minimum requirements for installing Bitdefender, you will be informed of the areas that need improvement before you can proceed.

If an incompatible antivirus program or an older version of Bitdefender is detected, you will be prompted to remove it from your system. Please follow the directions to remove the software from your system, thus avoiding problems occurring later on.



## Note

You may need to reboot your computer to complete the removal of detected antivirus programs.

Follow the setup wizard steps to install Bitdefender Antivirus Plus 2012.

## Step 1 - Welcome

Please read the License Agreement and select **Agree & Continue**. The License Agreement contains the terms and conditions under which you may use Bitdefender Antivirus Plus 2012.



## Note

If you do not agree to these terms, close the window. The installation process will be abandoned and you will exit setup.

## Step 2 - Register your product

To complete the registration of your product you need to enter a license key and create a MyBitdefender account. An active Internet connection is required.

Proceed according to your situation:

### ● I purchased the product

In this case, register the product by following these steps:

1. Select **I purchased the product and I want to register now**.
2. Type the license key in the corresponding field.



## Note

You can find your license key:

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

3. Type your e-mail address in the corresponding field.



## Important

A valid e-mail address is required. A confirmation message will be sent to the address you provided.

4. Click **Register Now**.

### ● I want to evaluate Bitdefender

In this case, you can use the product for a 30 day period. To begin the trial period, select **I want to evaluate this product**.

To use the online features of the product, you need to create a MyBitdefender account. To create an account, type your e-mail address in the corresponding field. A confirmation message will be sent to the address you provided. If you already have an account, enter the e-mail address associated with it to register the product to that account.

## Custom settings

Optionally, during this step you can customize the installation settings by clicking **Custom Settings**.

### Installation Path

By default, Bitdefender Antivirus Plus 2012 will be installed in C:\Program Files\Bitdefender\Bitdefender 2012. If you want to change the installation path, click **Change** and select the folder in which you would like Bitdefender to be installed.

### Configure Proxy Settings

Bitdefender Antivirus Plus 2012 requires access to the Internet for product registration, downloading security and product updates, in-cloud detection components etc. If you use a proxy connection instead of a direct Internet connection, you must select this option and configure the proxy settings.

The settings can be imported from the default browser or you can enter them manually.

### Enable P2P Update

You can share the product files and signatures with other Bitdefender users. This way, Bitdefender updates can be performed faster. If you don't want to enable this feature, select the corresponding check box.



## Note

No personal identifiable information will be shared if this feature is enabled.

If you want to minimize the impact of the network traffic on system performance during updates, use the update sharing option. Bitdefender uses ports 8880 - 8889 for peer-to-peer update.

## Send Anonymous Usage Reports

By default, Anonymous Usage Reports are enabled. By enabling this option, reports containing information about how you use the product are sent to Bitdefender servers. This information is essential for improving the product and can help us offer you a better experience in the future. Please note that these reports will contain no confidential data, such as your name or IP address, and that they will not be used for commercial purposes.

Click **OK** to confirm your preferences.

Click **Install** to start the installation.

## Step 3 - Installation progress

Wait for the installation to complete. Detailed information about the progress is displayed.

Critical areas on your system are scanned for viruses, the latest versions of the application files are downloaded and installed, and the Bitdefender services are started. This step can take a couple of minutes.

## Step 4 - Finish

A summary of the installation is displayed. If any active malware was detected and removed during the installation, a system reboot may be required.

Click **Finish**.

### 1.3.1. Upgrading from an older version

If you are already using an older version of Bitdefender, there are two ways to upgrade to Bitdefender Antivirus Plus 2012:

- Install Bitdefender Antivirus Plus 2012 directly over the older version. Bitdefender will detect the older version and will help you remove it before installing the new version. You will need to restart the computer during the upgrade.
- Remove the older version, then restart the computer and install the new version as described in the previous pages. Use this upgrade method if the other fails.



#### Note

Product settings and quarantine contents will not be imported from the older version.

## 2. Getting started

Once you have installed Bitdefender Antivirus Plus 2012, your computer is protected against all kinds of malware (such as viruses, spyware and trojans).

The **Auto Pilot** is by default engaged and you are not required to configure any settings. However, you may want to take advantage of the Bitdefender settings to fine-tune and improve your protection.

Bitdefender will make most security-related decisions for you and will rarely show pop-up alerts. Details about actions taken and information about program operation are available in the Events window. For more information, please refer to *“Events”* (p. 12).

From time to time, you should open Bitdefender and fix the existing issues. You may have to configure specific Bitdefender components or take preventive actions to protect your computer and your data.

If you have not registered the product (including creating a MyBitdefender account), remember to do so until the trial period ends. You must create an account in order to use the online features of the product. For more information about the registration process, please refer to *“Product registration”* (p. 7).

### 2.1. Opening Bitdefender

To access the main interface of Bitdefender Antivirus Plus 2012, use the Windows Start menu, by following the path **Start** → **All Programs** → **Bitdefender 2012** → **Bitdefender Antivirus Plus 2012** or, quicker, double-click the Bitdefender icon



in the system tray.

For more information about the Bitdefender window and icon in the system tray, please refer to *“Bitdefender interface”* (p. 18).

### 2.2. What you have to do after installation

If you want Bitdefender to handle all security-related decisions for you, keep the Auto Pilot engaged. For more information, please refer to *“Auto Pilot”* (p. 12).

Here is a list of tasks you may want to perform after you install:

- If your computer connects to the Internet through a proxy server, you must configure the proxy settings as described in *“How do I configure Bitdefender to use a proxy Internet connection?”* (p. 30).
- If you have installed Bitdefender on several computers in your home network, you can manage all Bitdefender products remotely from a single computer. For more information, please refer to *“Network Map”* (p. 62).

- Create Data Protection rules to prevent your important personal data from being disclosed without your consent. For more information, please refer to *“Data Protection”* (p. 58).

## 2.3. Product registration

In order to be protected by Bitdefender, you must register your product by entering a license key and creating a MyBitdefender account.

The license key specifies how long you may use the product. As soon as the license key expires, Bitdefender stops performing its functions and protecting your computer.

You should purchase a license key or renew your license a few days before the current license key expires. For more information, please refer to *“Buying or renewing license keys”* (p. 10). If you are using a trial version of Bitdefender, you must register it with a license key if you want to continue using it after the trial period ends.

A MyBitdefender account gives you access to product updates and allows you to use the online services offered by Bitdefender Antivirus Plus 2012. If you already have an account, register your Bitdefender product to that account.

A MyBitdefender account allows you to:

- Keep your product up to date.
- Recover your license key, should you ever lose it.
- Contact Bitdefender Customer Care.
- Get protection for your Facebook account with **Safego**.

### 2.3.1. Entering your license key

If, during the installation, you selected to evaluate the product, you can use it for a 30-day trial period. To continue using Bitdefender after the trial period expires, you must register it with a license key.

To register the product with a license key or change the current license key, click the **License Info** link, located at the bottom of the Bitdefender window. The registration window will appear.

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

To register Bitdefender Antivirus Plus 2012:

1. Type the license key in the edit field.



#### Note

You can find your license key:

- on the CD label.
- on the product registration card.

● in the online purchase e-mail.

If you do not have a Bitdefender license key, click the link provided in the window to open a web page from where you can purchase one.

2. Click **Register Now**.

## 2.3.2. Logging in to MyBitdefender

If you provided an e-mail address during the installation, a confirmation e-mail was sent to the address you provided. Click the link in the e-mail to complete the registration.

If you have not completed the registration, Bitdefender will notify you that you need to do so.



### Important

You must log in to an account within 30 days after installing Bitdefender. Otherwise, Bitdefender will no longer update.

To create or log in to a MyBitdefender account, click the **Complete registration / MyBitdefender** link, located at the bottom of the Bitdefender window.

The MyBitdefender window will open. Proceed according to your situation.

## I want to create a MyBitdefender account

To successfully create a MyBitdefender account, follow these steps:

1. Select **Create new account**.

A new window will appear.

2. Type the required information in the corresponding fields. The data you provide here will remain confidential.

● **Name** - enter a user name for your account. This field is optional.

● **E-mail** - enter your e-mail address.

● **Password** - enter a password for your account. The password must be at least 6 characters long.

● **Confirm password** - retype the password.

● Optionally, Bitdefender can inform you about special offers and promotions using the e-mail address of your account. To enable this option, select **I allow Bitdefender to send me e-mails**.



### Note

Once the account is created, you can use the provided e-mail address and password to log in to your account at <http://my.bitdefender.com>.

3. Click **Submit**.
4. Before being able to use your account, you must complete the registration. Check your e-mail and follow the instructions in the confirmation e-mail sent by Bitdefender.



## Note

You can also log in using your Facebook or Google account. For more information, please refer to ["I want to log in using my Facebook or Google account"](#) (p. 9)

## I want to log in using my Facebook or Google account

To log in with your Facebook or Google account, follow these steps:

1. Click the icon of the service you want to use to log in. You will be redirected to the login page of that service.
2. Follow the instructions provided by the selected service to link your account to Bitdefender.



## Note

Bitdefender does not get access to any confidential information such as the password of the account you use to log in, or the personal information of your friends and contacts.

## I already have a MyBitdefender account

If you have logged in to an account from your product before, Bitdefender will detect it and log you in to that account. You can visit your account at <http://my.bitdefender.com> by clicking **Go to MyBitdefender**.

If you want to log in to a different account, click the corresponding link and follow the instructions in the previous sections.

If you already have an active account, but Bitdefender does not detect it, follow these steps to log in to that account:

1. Type the e-mail address and the password of your account in the corresponding fields.



## Note

If you have forgotten your password, click **Forgot password** and follow the instructions to retrieve it.

2. Click **Login**.

## 2.3.3. Buying or renewing license keys

If the trial period is going to end soon, you must purchase a license key and register your product. Similarly, if your current license key is going to expire soon, you must renew your license.

Bitdefender will alert you when the expiration date of your current license is approaching. Follow the instructions in the alert to purchase a new license.

You can visit a web page from where a license key can be purchased at any time, by following these steps:

1. Open the Bitdefender window.
2. Click the **License Info** link, located at the bottom of the Bitdefender window, to open the product registration window.
3. Click the provided link on the lower part of the window.

## 2.4. Fixing issues

Bitdefender uses an issue tracking system to detect and inform you about the issues that may affect the security of your computer and data. By default, it will monitor only a series of issues that are considered to be very important. However, you can configure it as needed, choosing which specific issues you want to be notified about.

Detected issues include important protection settings that are turned off and other conditions that can represent a security risk. They are grouped into two categories:

- **Critical issues** - prevent Bitdefender from protecting you against malware or represent a major security risk.
- **Minor (non-critical) issues** - can affect your protection in the near future.

The Bitdefender icon in the **system tray** indicates pending issues by changing its color as follows:

**B Red color:** Critical issues affect the security of your system. They require your immediate attention and must be fixed as soon as possible.

**B Yellow color:** Non-critical issues affect the security of your system. You should check and fix them when you have the time.

Also, if you move the mouse cursor over the icon, a pop-up will confirm the existence of pending issues.

When you open the Bitdefender window, the Security status area on the upper toolbar will indicate the number and nature of issues affecting your system.

### 2.4.1. Fix All Issues wizard

To fix detected issues follow the **Fix All Issues** wizard.



1. To open the wizard, do any of the following:

- Right-click the Bitdefender icon in the **system tray** and choose **Fix All Issues**. Depending on the detected issues, the icon is either red **B** (indicating critical issues) or yellow **B** (indicating non-critical issues).
- Open the Bitdefender window and click anywhere inside the Security status area on the upper toolbar (for example, you can click the **Fix All Issues** button).

2. You can see the issues affecting the security of your computer and data. All current issues are selected to be fixed.

If you do not want to fix a specific issue right away, clear the corresponding check box. You will be prompted to specify for how long to postpone fixing the issue. Choose the desired option from the menu and click **OK**. To stop monitoring the respective issue category, choose **Permanently**.

The issue status will change to **Postpone** and no action will be taken to fix the issue.

3. To fix the selected issues, click **Start**. Some issues are fixed immediately. For others, a wizard helps you fix them.

The issues that this wizard helps you fix can be grouped into these main categories:

- **Disabled security settings.** Such issues are fixed immediately, by enabling the respective security settings.
- **Preventive security tasks you need to perform.** When fixing such issues, a wizard helps you successfully complete the task.

## 2.4.2. Configuring status alerts

The status alert system is pre-configured to monitor and alert you about the most important issues that may affect the security of your computer and data. Besides the issues monitored by default, there are several other issues you can be informed about.

You can configure the alert system to best serve your security needs by choosing which specific issues to be informed about. Follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **General** on the left-side menu and then the **Advanced** tab.
4. Look for and click the **Configure status alerts** link.
5. Click the switches to turn on or off status alerts according to your preferences.

## 2.5. Events

Bitdefender keeps a detailed log of events concerning its activity on your computer. Events are a very important tool in monitoring and managing your Bitdefender protection. For instance, you can easily check if the update was successfully performed, if malware was found on your computer etc. Additionally, you can take further action if needed or change actions taken by Bitdefender.

To open the Events window, open the Bitdefender window and click the **Events** button on the upper toolbar.


In order to help you filter the Bitdefender events, the following categories are available on the left-side menu:

- **Antivirus**
- **Privacy Control**
- **Network Map**
- **Update**
- **SafeGo**
- **Registration**

A list of events is available for each category. To find out information about a particular event in the list, click it. Event details are displayed in the lower part of the window. Each event comes with the following information: a short description, the action Bitdefender took on it when it happened, and the date and time when it occurred. Options may be provided to take further action if needed.

You can filter events by their importance. There are three types of events, each type indicated by a specific icon:

 **Information** events indicate successful operations.

 **Warning** events indicate non-critical issues. You should check and fix them when you have the time.

 **Critical** events indicate critical issues. You should check them immediately.

To help you easily manage logged events, each section of the Events window provides options to delete or mark as read all events in that section.


## 2.6. Auto Pilot

For all the users who want nothing more from their security solution than to be protected without being bothered, Bitdefender Antivirus Plus 2012 has been designed with a built-in Auto Pilot mode.

While on Auto Pilot, Bitdefender applies an optimal security configuration and takes all security-related decisions for you. This means you will see no pop-ups, no alerts and you will not have to configure any settings whatsoever.

In Auto Pilot mode, Bitdefender automatically fixes critical issues and quietly manages:

- Antivirus protection, provided by on-access scanning and continuous scanning.
- Firewall protection.
- Privacy protection, provided by antiphishing and antimalware filtering for your web browsing.
- Automatic updates.

By default, the Auto Pilot is engaged the moment the Bitdefender installation is completed. As long as Auto Pilot is engaged, the Bitdefender icon in the system tray will change to .

To turn the Auto Pilot on or off, open the Bitdefender window and click the **Auto Pilot** switch on the upper toolbar.



### Important

While the Auto Pilot is on, modifying any of the settings it manages will result in it being turned off.

To see a history of actions performed by Bitdefender while Auto Pilot was engaged, open the **Events** window.

## 2.7. Game Mode and Laptop Mode

Some computer activities, such as games or presentations, require increased system responsiveness and performance, and no interruptions. When your laptop is running on battery power, it is best that unnecessary operations, which consume additional power, be postponed until the laptop is connected back to A/C power.


To adapt to these particular situations, Bitdefender Antivirus Plus 2012 includes two special operation modes:

- **Game Mode**
- **Laptop Mode**

### 2.7.1. Game Mode

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

- All Bitdefender alerts and pop-ups are disabled.
- Auto Scan is turned off. Auto Scan finds and uses time-slices when system resource usage falls below a certain threshold to perform recurring scans of the entire system.
- Auto Update is turned off.
- The Bitdefender toolbar in your web browser is disabled when you play browser-based online games.

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

## Using Game Mode

By default, Bitdefender automatically enters Game Mode when you start a game from the Bitdefender's list of known games or when an application goes to full screen. Bitdefender will automatically return to the normal operation mode when you close the game or when the detected application exits full screen.

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

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



### Important

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

## Changing the Game Mode hotkey

You can manually enter Game Mode using the default **Ctrl+Alt+Shift+G** hotkey. If you want to change the hotkey, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **General** on the left-side menu and then the **Settings** tab.
4. Under the **Enable Game Mode hotkey** option, set the desired hotkey:
  - a. Choose the modifier keys you want to use by checking one the following: Control key (**Ctrl**), Shift key (**Shift**) or Alternate key (**Alt**).
  - b. In the edit field, type the letter corresponding to the regular key you want to use.

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



### Note

To disable the hotkey, turn off the **Enable Game Mode hotkey** option.

## Turning on or off automatic game mode

To turn on or off automatic game mode, follow these steps:

1. Open the Bitdefender window.

2. Click the **Settings** button on the upper toolbar.
3. Click **General** on the left-side menu and then the **Settings** tab.
4. Turn on or off automatic game mode by clicking the corresponding switch.

## 2.7.2. Laptop Mode

Laptop Mode is especially designed for laptop and notebook users. Its purpose is to minimize Bitdefender's impact on power consumption while these devices are running on battery. When Bitdefender operates in Laptop Mode, the Auto Scan and Auto Update features are turned off, as they require more system resources and, implicitly, increase power consumption.

Bitdefender detects when your laptop has switched to battery power and it automatically enters Laptop Mode. Likewise, Bitdefender automatically exits Laptop Mode, when it detects the laptop is no longer running on battery.

To turn on or off automatic laptop mode, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **General** on the left-side menu and then the **Settings** tab.
4. Turn on or off automatic laptop mode by clicking the corresponding switch.

If Bitdefender is not installed on a laptop, turn off automatic laptop mode.

## 2.8. Password-protecting Bitdefender settings

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

To configure password protection for the Bitdefender settings, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **General** on the left-side menu and then the **Settings** tab.
4. In the **Password-protect settings** section, turn on password protection by clicking the switch.
5. Click the **Change password** link.
6. Enter the password in the two fields and then click **OK**. The password must be at least 8 characters long.

Once you have set a password, anyone trying to change the Bitdefender settings will first have to provide the password.



## Important

Be sure to remember your password or keep a record of it in a safe place. If you forget the password, you will have to reinstall the program or to contact Bitdefender for support.

To remove password protection, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **General** on the left-side menu and then the **Settings** tab.
4. In the **Password-protect settings** section, turn off password protection by clicking the switch.
5. Enter the password and then click **OK**.

## 2.9. Anonymous usage reports

By default, Bitdefender sends reports containing information about how you use it to Bitdefender servers. This information is essential for improving the product and can help us offer you a better experience in the future. Please note that these reports will contain no confidential data, such as your name or IP address, and that they will not be used for commercial purposes.

In case you want to stop sending Anonymous usage reports, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **General** on the left-side menu and then the **Advanced** tab.
4. Turn off Anonymous usage reports by clicking the corresponding switch.

## 2.10. Repairing or removing Bitdefender

If you want to repair or remove Bitdefender Antivirus Plus 2012, follow the path from the Windows start menu: **Start** → **All Programs** → **Bitdefender 2012** → **Repair or Remove**.

Select the action you want to perform:

- **Repair** - to re-install all program components.
- **Remove** - to remove all installed components.



## Note

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

Wait for Bitdefender to complete the action you have selected. This will take several minutes.

You will need to restart the computer to complete the process.

## 3. Bitdefender interface

Bitdefender Antivirus Plus 2012 meets the needs of computer beginners and very technical people alike. Its graphical user interface is designed to suit each and every category of users.

To see the status of the product and perform essential tasks, the Bitdefender **system tray icon** is available at any time.

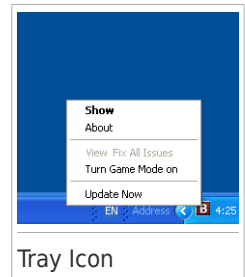
The **main window** gives you quick access to the product modules and important product information, and lets you perform common tasks.

To configure your Bitdefender product in detail and perform advanced administrative tasks, you can find all the tools you need in the **settings window**.

### 3.1. System tray icon

To manage the entire product more quickly, you can use the Bitdefender icon **B** in the system tray. If you double-click this icon, Bitdefender will open. Also, by right-clicking the icon, a contextual menu will allow you to quickly manage the Bitdefender product.

- **Show** - opens the main window of Bitdefender.
- **About** - opens a window where you can see information about Bitdefender and where to look for help in case something unexpected appears.
- **Fix All Issues** - helps you remove current security vulnerabilities. If the option is unavailable, there are no issues to be fixed. For detailed information, please refer to *"Fixing issues"* (p. 10).
- **Turn Game Mode On / Off** - activates / deactivates **Game Mode**.
- **Update Now** - starts an immediate update. You can follow the update status in the Update panel of the main Bitdefender window.



The Bitdefender system tray icon informs you when issues affect your computer or how the product operates, by displaying a special symbol, as follows:

**B** Critical issues affect the security of your system. They require your immediate attention and must be fixed as soon as possible.


**B** Non-critical issues affect the security of your system. You should check and fix them when you have the time.

**B** The product operates in **Game Mode**.



 Bitdefender **Auto Pilot** is engaged.

If Bitdefender is not working, the system tray icon appears on a gray background:

. This usually happens when the license key expires. It can also occur when the Bitdefender services are not responding or when other errors affect the normal operation of Bitdefender.

## 3.2. Main window

The main Bitdefender window allows you to perform common tasks, quickly fix security Issues, view information about events in product operation and customize product settings. Everything is just a few clicks away.

The window is organized in two main areas:


### Upper toolbar

This is where you can check your computer's security status and access important tasks.

### Panels area

This is where you can manage the main Bitdefender modules.

Additionally, you can find several useful links on the lower part of the window:

Link	Description
<b>Feedback</b>	Opens a web page in your browser where you can take a short survey about your experience in using the product. We rely on your feedback in our constant quest to improve Bitdefender products.
<b>Complete registration / MyBitdefender</b>	Opens the MyBitdefender account window, where you can create or log in to an account. A MyBitdefender account is required in order to receive updates and benefit from the online features of your product. To find out more about how you can create an account and the benefits it offers, please refer to <i>"Logging in to MyBitdefender"</i> (p. 8).
<b>License Info</b>	Opens a window where you can see current license key information and register your product with a new license key.
<b>Help and Support</b>	Click this link if you need help with Bitdefender.
	Adds question marks in different areas of the Bitdefender window to help you easily find information about the different interface elements.  Move your mouse cursor over a mark to see quick information about the element next to it.


## 3.2.1. Upper toolbar

The upper toolbar contains the following elements:

- **Security Status Area** on the left side of the toolbar, informs you if there are any issues affecting your computer's security and helps you fix them.

The color of the security status area changes depending on the detected issues and different messages are displayed:

- ▶ **The area is colored green.** There are no issues to fix. Your computer and data are protected.
- ▶ **The area is colored yellow.** Non-critical issues are affecting the security of your system. You should check and fix them when you have the time.
- ▶ **The area is colored red.** Critical issues are affecting the security of your system. You should address these issues immediately.

By clicking the **View Issues**  button in the center of the toolbar or anywhere in the security status area to its left, you can access a wizard that will help you easily remove any threats from your computer. For detailed information, please refer to *"Fixing issues"* (p. 10).

- **Events** allows you to access a detailed history of relevant events that occurred in the activity of the product. For detailed information, please refer to *"Events"* (p. 12).
- **Settings** allows you to access the settings window from where you can configure the product settings. For detailed information, please refer to *"Settings window"* (p. 22).
- **Auto Pilot** allows you to engage the Auto Pilot and enjoy completely silent security. For detailed information, please refer to *"Auto Pilot"* (p. 12).

## 3.2.2. Panels area

The panels area is where you can directly manage the Bitdefender modules.

You can organize the panels as you wish. To rearrange the area according to your needs, drag individual panels and drop them in other slots.

To browse through the panels, use the slider below the panels area or the arrows located to the right and to the left.

From top to bottom, each module panel contains the following elements:

- The name of the module.
- A status message.
- The icon of the module. Click the icon of a module to configure its settings in the *settings window*.

- A button that lets you perform important tasks related to the module.
- A switch is available on certain panels allowing you to turn on or off an important feature of the module.

The panels available in this area are:

## Antivirus

Antivirus protection is the foundation of your security. Bitdefender protects you in real-time and on-demand against all sorts of malware, such as viruses, trojans, spyware, adware, etc.

From the Antivirus panel you can easily access important scan tasks. Click **Scan Now** and select a task from the drop-down menu:

- Quick Scan
- Full System Scan
- Custom Scan
- Vulnerability Scan
- Rescue Mode

The **Auto Scan** switch allows you to turn the Auto Scan feature on or off.

For more information about scan tasks and how to configure antivirus protection, please refer to *"Antivirus protection"* (p. 32).

## Update

In a world where cyber criminals constantly try to come up with new ways to cause harm, it is essential to keep your security solution up to date if you are to stay one step ahead of them.

By default, Bitdefender automatically checks for updates every hour. If you want to turn off automatic updates, use the **Auto Update** switch on the Update panel.



### Warning

This is a critical security issue. We recommend you to disable automatic update for as little time as possible. If Bitdefender is not updated regularly, it will not be able to protect you against the latest threats.

Click the **Update Now** button on the panel to start an immediate update.

For more information about configuring updates, please refer to *"Update"* (p. 66).

## Privacy Control

The privacy control module helps you keep important personal data private. It protects you while on the Internet against phishing attacks, fraud attempts, private data leaks, and more.

Click the **Manage rules** button on the Privacy Control panel to go to the Data Protection section where you can configure privacy rules.

The Antiphishing switch allows you to turn on or off antiphishing protection.

For more information about how to configure Bitdefender to protect your privacy, please refer to *"Privacy Control"* (p. 55).

## Network Map

With Network Map you can easily manage the security of the computers in your home from a single computer.

To get started, click **Manage** on the Network Map panel and select **Enable network**.

Once the network is enable, clicking **Manage** on the Network Map panel will give you access to the following options.

- **Disable connection** - disable the network.
- **Scan all** - start a quick scan of full system scan on the managed computers.
- **Update all computers** - update the Bitdefender products on the managed computers.

For more information, please refer to *"Network Map"* (p. 62).

## Safego

To help you stay safe on Facebook, you can access Safego, the Bitdefender security solution for social networks, directly from your product.

Click **Activate** to activate and manage Safego from your Facebook account.

If you already activated Safego, you will be able to access statistics regarding its activity by clicking the **View Reports** button.

For more information, please refer to *"Safego protection for social networks"* (p. 70).

## 3.3. Settings window

The settings window gives you access to every product component and customization. This is where you can configure Bitdefender in detail.

On the left side of the window there is a menu containing all security modules. Each module has one or more tabs where you can configure the corresponding security settings or perform security or administrative tasks. The following list briefly describes each module.

### General

Allows you to configure general product settings, such as settings password, Game Mode, Laptop Mode, proxy settings and status alerts.

## Antivirus

Allows you to configure your protection against malware, detect and fix vulnerabilities of your system, set scan exclusions and manage quarantined files.

## Privacy Control

Allows you to prevent data theft from your computer and protect your privacy while you are online. Configure protection for your web browser, instant messaging software, manage data protection, and more.


## Network Map

Allows you to configure and manage the Bitdefender products installed on your home computers from a single computer.

## Update

Allows you to obtain info on the latest updates, to update the product and to configure the update process in detail.

Additionally, you can find several useful links on the lower part of the window:

Link	Description
<b>Feedback</b>	Opens a web page in your browser where you can take a short survey about your experience in using the product. We rely on your feedback in our constant quest to improve Bitdefender products.
<b>Complete registration / MyBitdefender</b>	Opens the MyBitdefender account window, where you can create or log in to an account. A MyBitdefender account is required in order to receive updates and benefit from the online features of your product. To find out more about how you can create an account and the benefits it offers, please refer to <i>"Logging in to MyBitdefender"</i> (p. 8).
<b>License Info</b>	Opens a window where you can see current license key information and register your product with a new license key.
<b>Help and Support</b>	Click this link if you need help with Bitdefender.
	Adds question marks in different areas of the Bitdefender window to help you easily find information about the different interface elements.  Move your mouse cursor over a mark to see quick information about the element next to it.

To return to the **main window**, click the **Home** button in the upper-right corner of the window.

## 4. How to

This chapter provides step-by-step instructions to configure commonly used settings or to complete common tasks with Bitdefender. Some of the topics include references to other topics where you can find detailed information.

- [“How do I register a trial version?”](#) (p. 24)
- [“How do I register Bitdefender without an Internet connection?”](#) (p. 25)
- [“How do I upgrade to another Bitdefender 2012 product?”](#) (p. 26)
- [“When should I reinstall Bitdefender?”](#) (p. 26)
- [“When does my Bitdefender protection expire?”](#) (p. 26)
- [“How do I renew my Bitdefender protection?”](#) (p. 27)
- [“What Bitdefender product am I using?”](#) (p. 27)
- [“How do I scan a file or a folder?”](#) (p. 28)
- [“How do I scan my system?”](#) (p. 28)
- [“How do I create a custom scan task?”](#) (p. 28)
- [“How do I exclude a folder from being scanned?”](#) (p. 28)
- [“What to do when Bitdefender detected a clean file as infected?”](#) (p. 29)
- [“How do I protect my personal information?”](#) (p. 30)
- [“How do I configure Bitdefender to use a proxy Internet connection?”](#) (p. 30)

### 4.1. How do I register a trial version?

If you have installed a trial version, you may only use it for a limited period of time. To continue using Bitdefender after the trial period expires, you must register your product with a license key and create a MyBitdefender account.

- To register Bitdefender, follow these steps:
  1. Open the Bitdefender window.
  2. Click the **License Info** link at the bottom of the window. The registration window will appear.
  3. Enter the license key and click **Register Now**.

If you do not have a license key, click the link provided in the window to visit a web page from where you can purchase one.
  4. Wait until the registration process is completed and close the window.
- To create a MyBitdefender account, follow these steps:
  1. Open the Bitdefender window.

2. Click the **Complete registration** link at the bottom of the window. The account window will appear.
3. Select the corresponding link to create a new account.
4. Type the required information in the corresponding fields. The data you provide here will remain confidential.

Click **Submit**.

5. Check your e-mail and follow the instructions received in order to complete the registration.



## Note

You can use the provided e-mail address and password to log in to your account at <http://my.bitdefender.com>.

## 4.2. How do I register Bitdefender without an Internet connection?

If you just purchased Bitdefender and you do not have an Internet connection, you can still register Bitdefender offline.

To register Bitdefender with your license key, follow these steps:

1. Go to a PC connected to the Internet. For example, you can use a friend's computer or a PC from a public location.
2. Go to <https://my.bitdefender.com> to create a MyBitdefender account.
3. Log in to your account and select **Obtain offline registration**.
4. Enter the license key you purchased.
5. Click **Submit** to obtain a confirmation code.



## Important

Write down the confirmation code.

6. Go back to your PC with the confirmation code.
7. Open the Bitdefender window.
8. Click the **License Info** link at the bottom of the window. The registration window will appear.
9. Select the option to register the product with a confirmation code.
10. Enter the confirmation code in the corresponding field and click **Submit**.
11. Wait until the registration process is completed and click **Finish**.

## 4.3. How do I upgrade to another Bitdefender 2012 product?

You can easily upgrade from one Bitdefender 2012 product to another.

Let's consider the following scenario: you have been using Bitdefender Antivirus Plus 2012 for a while and recently you have decided to go for Bitdefender Total Security 2012 and the extra features it offers.

All you need to do is purchase a license key for the Bitdefender 2012 product you want to upgrade to and enter it in the registration window of the Bitdefender 2012 product you are currently using.

Follow these steps:

1. Open the Bitdefender window.
2. Click the **License Info** link at the bottom of the window. The registration window will appear.
3. Enter the license key and click **Register Now**.
4. Bitdefender will inform you that the license key is for a different product and will give you the option to install it. Click the corresponding link and follow the procedure to perform the upgrade.

## 4.4. When should I reinstall Bitdefender?

In some situations, you may need to reinstall your Bitdefender product.

Typical situations when you would need to reinstall Bitdefender include the following:

- you have reinstalled the operating system
- you have purchased a new computer
- you want to change the display language of the Bitdefender interface

To reinstall Bitdefender you can use the installation disc you purchased or download a new version from the [Bitdefender website](#).

During the installation, you will be asked to register the product with your license key.

If you cannot find your license key, you can log in to <https://my.bitdefender.com> to retrieve it. Type the e-mail address and the password of your account in the corresponding fields.

## 4.5. When does my Bitdefender protection expire?

To find out the remaining number of days from your license key, follow these steps:

1. Open the Bitdefender window.
2. Click the **License Info** link at the bottom of the window.



3. In the **Register your product** window you can notice the remaining number of days.

## 4.6. How do I renew my Bitdefender protection?

When your Bitdefender protection is about to expire, you must renew your license key.

- Follow these steps to visit a website where you can renew your Bitdefender license key:
  1. Open the Bitdefender window.
  2. Click the **License Info** link at the bottom of the window.
  3. Click **Don't have a license key? Buy one now!**
  4. A web page will open on your web browser where you can purchase a Bitdefender license key.



### Note

As an alternative, you can contact the retailer you bought your Bitdefender product from.

- Follow these steps to register your Bitdefender with the new license key:
  1. Open the Bitdefender window.
  2. Click the **License Info** link at the bottom of the window. The registration window will appear.
  3. Enter the license key and click **Register Now**.
  4. Wait until the registration process is completed and close the window.

For more information, you can contact Bitdefender for support as described in section *"Support"* (p. 85).

## 4.7. What Bitdefender product am I using?

To find out which Bitdefender program you have installed, follow these steps:

1. Open the Bitdefender window.
2. At the top of the window you should see one of the following:
  - Bitdefender Antivirus Plus 2012
  - Bitdefender Internet Security 2012
  - Bitdefender Total Security 2012

## 4.8. How do I scan a file or a folder?

The easiest and recommended way to scan a file or folder is to right-click the object you want to scan and select **Scan with Bitdefender** from the menu. To complete the scan, follow the Antivirus Scan wizard.

Typical situations when you would use this scanning method include the following:

- You suspect a specific file or folder to be infected.
- Whenever you download from the Internet files that you think they might be dangerous.
- Scan a network share before copying files to your computer.

## 4.9. How do I scan my system?

To perform a full scan on the system, follow these steps:

1. Open the Bitdefender window.
2. Go to the **Antivirus** panel.
3. Click **Scan Now** and select **Full System Scan** from the drop-down menu.
4. Follow the Antivirus Scan wizard to complete the scan.

## 4.10. How do I create a custom scan task?

To create a customized scan task, proceed as follows:

1. Open the Bitdefender window.
2. Go to the **Antivirus** panel.
3. Click **Scan Now** and select **Custom Scan** from the drop-down menu.
4. Click **Add Target** to select the files or folders to be scanned.
5. If you want to configure the scanning options in detail, click **Scan Options**.

You may select the **Shutdown Computer** option.

If no threats are found during the scan, your computer will be shut down when the scan is over. Remember that this will be the default behavior everytime you run this task.

6. Click **Start Scan** to run the task.

## 4.11. How do I exclude a folder from being scanned?

Bitdefender allows excluding specific files, folders or file extensions from scanning.

Exclusions are to be used by users having advanced computer knowledge and only in the following situations:

- You have a large folder on your system where you keep movies and music.
- You have a large archive on your system where you keep different data.
- You keep a folder where you install different types of software and applications for testing purposes. Scanning the folder may result in losing some of the data.

To add the folder to the Exclusions list, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Exclusions** tab.
4. Click the **Excluded files and folders** link.
5. Click the **Add** button, located at the top of the exclusions table.
6. Click **Browse**, select the folder that you want to be excluded from scanning and then click **OK**.
7. Click **Add** and then click **OK** to save the changes and close the window.

## 4.12. What to do when Bitdefender detected a clean file as infected?

There are cases when Bitdefender mistakenly flags a legitimate file as being a threat (a false positive). To correct this error, add the file to the Bitdefender Exclusions area:

1. Turn off the Bitdefender real-time antivirus protection:
  - a. Open the Bitdefender window.
  - b. Click the **Settings** button on the upper toolbar.
  - c. Click **Antivirus** on the left-side menu and then the **Shield** tab.
  - d. Click the switch to turn off **on-access scanning**.
2. Display hidden objects in Windows. To find out how to do this, please refer to *"How do I display hidden objects in Windows?"* (p. 93).
3. Restore the file from the Quarantine area:
  - a. Open the Bitdefender window.
  - b. Click the **Settings** button on the upper toolbar.
  - c. Click **Antivirus** on the left-side menu and then the **Quarantine** tab.
  - d. Select the file and click **Restore**.
4. Add the file to the Exclusions list. To find out how to do this, please refer to *"How do I exclude a folder from being scanned?"* (p. 28).

5. Turn on the Bitdefender real-time antivirus protection.
6. Contact our support representatives so that we may remove the detection signature. To find out how to do this, please refer to *"Asking for help"* (p. 86).

## 4.13. How do I protect my personal information?

Privacy Control monitors the data leaving your computer through web forms, e-mail messages or instant messages.

To make sure no private data leaves your computer without your consent, you must create appropriate data protection rules and exceptions to these rules.

The data protection rules specify the information to be blocked.

To create a Data Protection rule, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Privacy Control** on the left-side menu and then the **Data Protection** tab.
4. If **Data Protection** is turned off, turn it on using the corresponding switch.
5. Select the **Add rule** option to start the Data Protection wizard.
6. Follow the wizard steps.

## 4.14. How do I configure Bitdefender to use a proxy Internet connection?

If your computer connects to the Internet through a proxy server, you must configure Bitdefender with the proxy settings. Normally, Bitdefender automatically detects and imports the proxy settings from your system.



### Important

Home Internet connections do not normally use a proxy server. As a rule of thumb, check and configure the proxy connection settings of your Bitdefender program when updates are not working. If Bitdefender can update, then it is properly configured to connect to the Internet.

To manage the proxy settings, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **General** on the left-side menu and then the **Advanced** tab.
4. In the **Proxy settings** section, turn on proxy usage by clicking the switch.
5. Click the **Manage proxies** link.

6. There are two options to set the proxy settings:

- **Import proxy settings from default browser** - proxy settings of the current user, extracted from the default browser. If the proxy server requires a username and a password, you must specify them in the corresponding fields.



#### Note

Bitdefender can import proxy settings from the most popular browsers, including the latest versions of Internet Explorer, Mozilla Firefox and Opera.

- **Custom proxy settings** - proxy settings that you can configure yourself. The following settings must be specified:
  - ▶ **Address** - type in the IP of the proxy server.
  - ▶ **Port** - type in the port Bitdefender uses to connect to the proxy server.
  - ▶ **User name** - type in a user name recognized by the proxy.
  - ▶ **Password** - type in the valid password of the previously specified user.

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

Bitdefender will use the available proxy settings until it manages to connect to the Internet.



#### Important

Remember to turn off proxy usage when you switch to a direct Internet connection.

## 5. Antivirus protection

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

- **On-access scanning** - prevents new malware threats from entering your system. Bitdefender will, for example, scan a word document for known threats when you open it, and an e-mail message when you receive one.

On-access scanning ensures real-time protection against malware, being an essential component of any computer security program.



### Important

To prevent viruses from infecting your computer keep **on-access scanning** enabled.

- **On-demand scanning** - allows detecting and removing the malware that already resides in the system. This is the classic scan initiated by the user - you choose what drive, folder or file Bitdefender should scan, and Bitdefender scans it - on-demand.

With **Auto Scan** turned on, there is hardly any need to manually run scans for malware. Auto Scan will scan your computer over and over again, taking appropriate actions when malware is detected. Auto Scan runs only when enough system resources are available so as not to slow down the computer.

Bitdefender automatically scans any removable media that is connected to the computer to make sure it can be safely accessed. For more information, please refer to *"Automatic scan of removable media"* (p. 44).

Advanced users can configure scan exclusions if they do not want specific files or file types to be scanned. For more information, please refer to *"Configuring scan exclusions"* (p. 46).

When it detects a virus or other malware, Bitdefender will automatically attempt to remove the malware code from the infected file and reconstruct the original file. This operation is referred to as disinfection. Files that cannot be disinfected are moved to quarantine in order to contain the infection. For more information, please refer to *"Managing quarantined files"* (p. 48).

If your computer has been infected with malware, please refer to *"Removing malware from your system"* (p. 77). To help you clean your computer of malware that cannot be removed from within the Windows operating system, Bitdefender provides you with **Rescue Mode**. This is a trusted environment, especially designed for malware removal, which enables you to boot your computer independent of Windows. When the computer runs in Rescue Mode, Windows malware is inactive, making it easy to remove.

To protect you against unknown malicious applications, Bitdefender uses Active Virus Control, an advanced heuristic technology, which continuously monitors the applications running on your system. Active Virus Control automatically blocks applications that exhibit malware-like behavior to stop them from damaging your computer. Occasionally, legitimate applications may be blocked. In such situations, you can configure Active Virus Control not to block those applications again by creating exclusion rules. To learn more, please refer to *"Active Virus Control"* (p. 49).

Many forms of malware are designed to infect systems by exploiting their vulnerabilities, such as missing operating system updates or outdated applications. Bitdefender helps you easily identify and fix system vulnerabilities in order to make your computer more secure against malware and hackers. For more information, please refer to *"Fixing system vulnerabilities"* (p. 51).

## 5.1. On-access scanning (real-time protection)

Bitdefender provides continuous, real-time protection against a wide range of malware threats by scanning all accessed files, e-mail messages and the communications through Instant Messaging Software applications (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

The default real-time protection settings ensure good protection against malware, with minor impact on system performance. You can easily change the real-time protection settings according to your needs by switching to one of the predefined protection levels. Or, if you are an advanced user, you can configure the scan settings in detail by creating a custom protection level.

### 5.1.1. Checking malware detected by on-access scanning

To check malware detected by on-access scanning, follow these steps:

1. Open the Bitdefender window.
2. Click the **Events** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Virus Scans** tab. This is where you can find all malware scan events, including threats detected by on-access scanning, user-initiated scans and status changes for automatic scans.
4. Click an event to view details about it.

### 5.1.2. Adjusting the real-time protection level

The real-time protection level defines the scan settings for real-time protection. You can easily change the real-time protection settings according to your needs by switching to one of the predefined protection levels.

To adjust the real-time protection level, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Shield** tab.
4. Drag the slider along the scale to set the desired protection level. Use the description on the right side of the scale to choose the protection level that better fits your security needs.

## 5.1.3. Creating a custom protection level

Advanced users might want to take advantage of the scan settings Bitdefender offers. You can configure the real-time protection settings in detail by creating a custom protection level.

To create a custom protection level, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Shield** tab.
4. Click **Custom**.
5. Configure the scan settings as needed.
6. Click **OK** to save the changes and close the window.

You may find this information useful:

- If you are not familiar with some of the terms, check them in the [glossary](#). You can also find useful information by searching the Internet.
- **Scan options for accessed files.** You can set Bitdefender to scan all accessed files or applications (program files) only. Scanning all accessed files provides best protection, while scanning applications only can be used for better system performance.

Applications (or program files) are far more vulnerable to malware attacks than other types of files. This category includes the following file extensions:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fpx; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx;



ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Scan inside archives.** Scanning inside archives is a slow and resource-intensive process, which is therefore not recommended for real-time protection. Archives containing infected files are not an immediate threat to the security of your system. The malware can affect your system only if the infected file is extracted from the archive and executed without having real-time protection enabled.

If you decide on using this option, you can set a maximum accepted size limit of archives to be scanned on-access. Select the corresponding check box and type the maximum archive size (in MB).

- **Scan options for e-mail, web and instant messaging traffic.** To prevent malware from being downloaded to your computer, Bitdefender automatically scans the following malware entry points:

- ▶ incoming and outgoing e-mails
- ▶ web traffic
- ▶ files received via Yahoo! Messenger and Windows Live Messenger

Scanning the web traffic may slow down web browsing a little, but it will block malware coming from the Internet, including drive-by downloads.

Though not recommended, you can disable e-mail, web or instant messaging antivirus scan to increase system performance. If you disable the corresponding scan options, the e-mails and files received or downloaded from the Internet will not be scanned, thus allowing infected files to be saved to your computer. This is not a major threat because real-time protection will block the malware when the infected files are accessed (opened, moved, copied or executed).

- **Scan boot sectors.** You can set Bitdefender to scan the boot sectors of your hard disk. This sector of the hard disk contains the necessary computer code to start the boot process. When a virus infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.
- **Scan only new and changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.

## 5.1.4. Restoring the default settings

The default real-time protection settings ensure good protection against malware, with minor impact on system performance.

To restore the default real-time protection settings, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Shield** tab.
4. Click **Default**.

## 5.1.5. Turning on or off real-time protection

To turn on or off real-time protection against malware, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Shield** tab.
4. Click the switch to turn on or off on-access scanning.
5. If you want to disable real-time protection, a warning window will appear. You must confirm your choice by selecting from the menu how long you want the real-time protection to be disabled. You can disable real-time protection for 5, 15 or 30 minutes, for an hour, permanently or until the system restart.



### Warning

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

## 5.1.6. Actions taken on detected malware

Files detected by real-time protection are grouped into two categories:

- **Infected files.** Files detected as infected match a malware signature in the Bitdefender Malware Signature Database. Bitdefender can normally remove the malware code from an infected file and reconstruct the original file. This operation is known as disinfection.



### Note

Malware signatures are snippets of code extracted from actual malware samples. They are used by antivirus programs to perform pattern-matching and detect malware.

The Bitdefender Malware Signature Database is a collection of malware signatures updated hourly by the Bitdefender malware researchers.

- **Suspicious files.** Files are detected as suspicious by the heuristic analysis. Because B-HAVE is a heuristic analysis technology, Bitdefender cannot be sure that the file is actually infected with malware. Suspicious files cannot be disinfected, because no disinfection routine is available.

Depending on the type of detected file, the following actions are taken automatically:

- If an infected file is detected, Bitdefender will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.



### Important

For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

- If a suspicious file is detected, it will be moved to quarantine to prevent a potential infection.

By default, quarantined files are automatically sent to Bitdefender Labs in order to be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

## 5.2. On-demand scanning

The main objective for Bitdefender is to keep your computer clean of viruses. This is first and foremost done by keeping new viruses out of your computer and by scanning your e-mail messages and any new files downloaded or copied to your system.

There is a risk that a virus is already lodged in your system, before you even install Bitdefender. This is why it's a very good idea to scan your computer for resident viruses after you've installed Bitdefender. And it's definitely a good idea to frequently scan your computer for viruses.

On-demand scanning is based on scan tasks. Scan tasks specify the scanning options and the objects to be scanned. You can scan the computer whenever you want by running the default tasks or your own scan tasks (user-defined tasks). If you want to scan specific locations on your computer or to configure the scan options, configure and run a custom scan.

### 5.2.1. Auto Scan

Auto Scan is a light on-demand scan that silently scans all your data for malware and takes the appropriate actions for any infections found. Auto Scan finds and uses time-slices when system resource usage falls below a certain threshold to perform recurring scans of the entire system.

Benefits of using Auto Scan:

- It has close to zero impact on the system.
- By pre-scanning the entire hard-disk, future on-demand tasks will be completed extremely fast.
- On-access scanning will also take significantly less time.

To turn on or off Auto Scan, follow these steps:

1. Open the Bitdefender window.
2. Go to the **Antivirus** panel.
3. Click the switch to turn on or off Auto Scan.

## 5.2.2. Scanning a file or folder for malware

You should scan files and folders whenever you suspect they might be infected. Right-click the file or folder you want to be scanned and select **Scan with Bitdefender**. The **Antivirus Scan wizard** will appear and guide you through the scanning process.

## 5.2.3. Running a Quick Scan

Quick Scan uses in-the-cloud scanning to detect malware running in your system. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.

To run a Quick Scan, follow these steps:

1. Open the Bitdefender window.
2. Go to the **Antivirus** panel.
3. Click **Scan now** and select **Quick Scan** from the drop-down menu.
4. Follow the **Antivirus Scan wizard** to complete the scan.

## 5.2.4. Running a Full System Scan

The Full System Scan task scans the entire computer for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others. If you have turned off **Auto Scan**, it is recommended to run a Full System Scan at least once a week.



### Note

Because **Full System Scan** performs a thorough scan of the entire system, the scan may take a while. Therefore, it is recommended to run this task when you are not using your computer.

Before running a Full System Scan, the following are recommended:

- Make sure Bitdefender is up-to-date with its malware signatures. Scanning your computer using an outdated signature database may prevent Bitdefender from detecting new malware found since the last update. For more information, please refer to *"Update"* (p. 66).
- Shut down all open programs.

If you want to scan specific locations on your computer or to configure the scanning options, configure and run a custom scan. For more information, please refer to *“Configuring and running a custom scan”* (p. 39).

To run a Full System Scan, follow these steps:

1. Open the Bitdefender window.
2. Go to the **Antivirus** panel.
3. Click **Scan now** and select **Full System Scan** from the drop-down menu.
4. Follow the **Antivirus Scan wizard** to complete the scan.

## 5.2.5. Configuring and running a custom scan

To configure a scan for malware in detail and then run it, follow these steps:

1. Open the Bitdefender window.
2. Go to the **Antivirus** panel.
3. Click **Scan now** and select **Custom Scan** from the drop-down menu.
4. Click **Add Target**, select the check boxes corresponding to the locations you want to be scanned for malware and then click **OK**.
5. Click **Scan Options** if you want to configure the scan options. A new window will appear. Follow these steps:

- a. You can easily configure the scanning options by adjusting the scan level. Drag the slider along the scale to set the desired scan level. Use the description on the right side of the scale to identify the scan level that better fits your needs.

Advanced users might want to take advantage of the scan settings Bitdefender offers. To configure the scan options in detail, click **Custom**. You can find information about them at the end of this section.

- b. By default, Bitdefender attempts to remove the malware code from infected files or, if disinfection fails, to move them to quarantine. If both of these actions fail, you will be prompted to specify an action to be taken on the unresolved threats.

If you want to only detect malware, without taking any other action, select the corresponding check box in the **Actions** section.

- c. You can also configure these general options:

- **Run the task with low priority.** Decreases the priority of the scan process. You will allow other programs to run faster and increase the time needed for the scan process to finish.
- **Minimize Scan Wizard to system tray.** Minimizes the scan window to the **system tray**. Double-click the Bitdefender icon to open it.

- Specify the action to be taken if no threats are found.
  - d. Click **OK** to save the changes and close the window.
6. Click **Start Scan** and follow the **Antivirus Scan wizard** to complete the scan. Depending on the locations to be scanned, the scan may take a while.

## Information on the scan options

You may find this information useful:

- If you are not familiar with some of the terms, check them in the **glossary**. You can also find useful information by searching the Internet.

- **Scan files.** You can set Bitdefender to scan all types of files or applications (program files) only. Scanning all files provides best protection, while scanning applications only can be used to perform a quicker scan.

Applications (or program files) are far more vulnerable to malware attacks than other types of files. This category includes the following file extensions: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fpx; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Scan options for archives.** Archives containing infected files are not an immediate threat to the security of your system. The malware can affect your system only if the infected file is extracted from the archive and executed without having real-time protection enabled. However, it is recommended to use this option in order to detect and remove any potential threat, even if it is not an immediate threat.



### Note

Scanning archived files increases the overall scanning time and requires more system resources.

- **Scan boot sectors.** You can set Bitdefender to scan the boot sectors of your hard disk. This sector of the hard disk contains the necessary computer code to start the boot process. When a virus infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.
- **Scan memory.** Select this option to scan programs running in your system's memory.
- **Scan registry.** Select this option to scan registry keys. Windows Registry is a database that stores configuration settings and options for the Windows operating system components, as well as for installed applications.
- **Scan cookies.** Select this option to scan the cookies stored by browsers on your computer.
- **Scan only new and changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.
- **Ignore commercial keyloggers.** Select this option if you have installed and use commercial keylogger software on your computer. Commercial keyloggers are legitimate computer monitoring software whose most basic function is to record everything that is typed on the keyboard.

## 5.2.6. Antivirus Scan Wizard

Whenever you initiate an on-demand scan (for example, right-click a folder and select **Scan with Bitdefender**), the Bitdefender Antivirus Scan wizard will appear. Follow the wizard to complete the scanning process.



### Note

If the scan wizard does not appear, the scan may be configured to run silently, in the background. Look for the **B** scan progress icon in the **system tray**. You can click this icon to open the scan window and to see the scan progress.

### Step 1 - Choose Scan Locations

This step appears only when you use Custom Scan. For more information, please refer to *"Configuring and running a custom scan"* (p. 39).

### Step 2 - Perform Scan

Bitdefender will start scanning the selected objects.

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

Wait for Bitdefender to finish scanning.



## Note

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

**Password-protected archives.** When a password-protected archive is detected, depending on the scan settings, you may be prompted to provide the password. Password-protected archives cannot be scanned unless you provide the password. The following options are available:

- **Enter password.** If you want Bitdefender to scan the archive, select this option and type the password. If you do not know the password, choose one of the other options.
- **Don't ask for a password and skip this object from scanning.** Select this option to skip scanning this archive.
- **Skip all password-protected items without scanning them.** Select this option if you do not want to be bothered about password-protected archives. Bitdefender will not be able to scan them, but a record will be kept in the scan log.

Click **OK** to continue scanning.

**Stopping or pausing the scan.** You can stop scanning anytime you want by clicking **Stop&Yes**. You will go directly to the last step of the wizard. To temporarily stop the scanning process, just click **Pause**. You will have to click **Resume** to resume scanning.

## Step 3 - Choose Actions

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

If there are no unresolved threats, click **Continue**. Otherwise, you must configure new actions to be taken on the unresolved threats in order to protect your system.

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

You can choose an overall action to be taken for all issues or you can select separate actions for each group of issues. One or several of the following options can appear on the menu:

### Take No Action

No action will be taken on the detected files. After the scan is completed, you can open the scan log to view information on these files.

### Disinfect

Removes the malware code from infected files.



## Delete

Removes detected files from the disk.

## Move to quarantine

Moves detected files to quarantine. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. For more information, please refer to *"Managing quarantined files"* (p. 48).

## Rename files

Changes the name of hidden files by appending .bd .ren to their name. As a result, you will be able to search for and find such files on your computer, if any.

Please note that these hidden files are not the files that you deliberately hide from Windows. They are the files hidden by special programs, known as rootkits. Rootkits are not malicious in nature. However, they are commonly used to make viruses or spyware undetectable by normal antivirus programs.

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

## Step 4 - Summary

When Bitdefender finishes fixing the issues, the scan results will appear in a new window. If you want comprehensive information on the scanning process, click **Show Log** to view the scan log.



### Important

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

Click **Close** to close the window.

## Bitdefender Could Not Solve Some Issues

In most cases Bitdefender successfully disinfects the infected files it detects or it isolates the infection. However, there are issues that cannot be solved automatically. For more information and instructions on how to remove malware manually, please refer to *"Removing malware from your system"* (p. 77).

## Bitdefender Detected Suspect Files

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

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

## 5.2.7. Checking scan logs

Each time you perform a scan, a scan log is created. The scan log contains detailed information about the logged scanning process, such as scanning options, the scanning target, the threats found and the actions taken on these threats.

You can open the scan log directly from the scan wizard, once the scan is completed, by clicking **Show Log**.

To check scan logs at a later time, follow these steps:

1. Open the Bitdefender window.
2. Click the **Events** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Virus Scans** tab. This is where you can find all malware scan events, including threats detected by on-access scanning, user-initiated scans and status changes for automatic scans.
4. In the events list, you can check what scans have been performed recently. Click an event to view details about it.
5. To open the scan log, click **View log**. The scan log will open in your default web browser.

## 5.3. Automatic scan of removable media


Bitdefender automatically detects when you connect a removable storage device to your computer and scans it in the background. This is recommended in order to prevent viruses and other malware from infecting your computer.

Detected devices fall into one of these categories:

- CDs/DVDs
- USB storage devices, such as flash pens and external hard-drives
- mapped (remote) network drives

You can configure automatic scan separately for each category of storage devices. Automatic scan of mapped network drives is off by default.

### 5.3.1. How does it work?

When it detects a removable storage device, Bitdefender starts scanning it for malware in the background (provided automatic scan is enabled for that type of device). A Bitdefender scan icon  will appear in the **system tray**. You can click this icon to open the scan window and to see the scan progress.

If Autopilot is on, you will not be bothered about the scan. The scan will only be logged and information about it will be available in the **Events** window.

If Autopilot is off:

1. You will be notified through a pop-up window that a new device has been detected and it is being scanned.
2. If a password-protected archive is detected during the scan, you may be prompted to provide the password. Password-protected archives cannot be scanned unless you provide the password. You can choose to enter the password, skip the file from scanning or disable detection of password-protected archives.
3. In most cases, Bitdefender automatically removes detected malware or isolates infected files into quarantine. If there are unresolved threats after the scan, you will be prompted to choose the actions to be taken on them.



## Note

Take into account that no action can be taken on infected or suspicious files detected on CDs/DVDs. Similarly, no action can be taken on infected or suspicious files detected on mapped network drives if you do not have the appropriate privileges.

4. When the scan is completed, the scan results window is displayed to inform you if you can safely access files on the removable media.

This information may be useful to you:

- Please be careful when using a malware-infected CD/DVD, because the malware cannot be removed from the disc (the media is read-only). Make sure real-time protection is turned on to prevent malware from spreading to your system. It is best practice to copy any valuable data from the disc to your system and then dispose of the disc.
- In some cases, Bitdefender may not be able to remove malware from specific files due to legal or technical constraints. Such an example are files archived using a proprietary technology (this is because the archive cannot be recreated correctly).

To find out how to deal with malware, please refer to *"Removing malware from your system"* (p. 77).

## 5.3.2. Managing removable media scan

To manage automatic scan of removable media, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Exclusions** tab.
4. In the **Scan detected devices** section, choose which types of storage devices you want to be scanned automatically. Click the switches to turn on or off automatic scan.

For best protection, it is recommended to turn on automatic scan for all types of removable storage devices.

The scanning options are pre-configured for the best detection results. If infected files are detected, Bitdefender will try to disinfect them (remove the malware code) or to move them to quarantine. If both actions fail, the Antivirus Scan wizard will allow you to specify other actions to be taken on infected files. The scanning options are standard and you cannot change them.

## 5.4. Configuring scan exclusions

Bitdefender allows excluding specific files, folders or file extensions from scanning. This feature is intended to avoid interference with your work and it can also help improve system performance. Exclusions are to be used by users having advanced computer knowledge or, otherwise, following the recommendations of a Bitdefender representative.

You can configure exclusions to apply to on-access or on-demand scanning only, or to both. The objects excluded from on-access scanning will not be scanned, no matter if they are accessed by you or by an application.



### Note

Exclusions will NOT apply for contextual scanning. Contextual scanning is a type of on-demand scanning: you right-click the file or folder you want to scan and select **Scan with Bitdefender**.

### 5.4.1. Excluding files or folders from scanning

To exclude specific files or folders from scanning, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Exclusions** tab.
4. Turn on scan exclusions for files using the corresponding switch.
5. Click the **Excluded files and folders** link. In the window that appears, you can manage the files and folders excluded from scanning.
6. Add exclusions by following these steps:
  - a. Click the **Add** button, located at the top of the exclusions table.
  - b. Click **Browse**, select the file or folder that you want to be excluded from scanning and then click **OK**. Alternatively, you can type (or copy and paste) the path to the file or folder in the edit field.

- c. By default, the selected file or folder is excluded from both on-access and on-demand scanning. To change when to apply the exclusion, select one of the other options.
  - d. Click **Add**.
7. Click **OK** to save the changes and close the window.

## 5.4.2. Excluding file extensions from scanning

When you exclude a file extension from scanning, Bitdefender will no longer scan files with that extension, regardless of their location on your computer. The exclusion also applies to files on removable media, such as CDs, DVDs, USB storage devices or network drives.



### Important

Use caution when excluding extensions from scanning because such exclusions can make your computer vulnerable to malware.

To exclude file extensions from scanning, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Exclusions** tab.
4. Turn on scan exclusions for files using the corresponding switch.
5. Click the **Excluded extensions** link. In the window that appears, you can manage the file extensions excluded from scanning.
6. Add exclusions by following these steps:
  - a. Click the **Add** button, located at the top of the exclusions table.
  - b. Enter the extensions that you want to be excluded from scanning, separating them with semicolons (;). Here is an example:  
`txt;avi;jpg`
  - c. By default, all files with the specified extensions are excluded from both on-access and on-demand scanning. To change when to apply the exclusion, select one of the other options.
  - d. Click **Add**.
7. Click **OK** to save the changes and close the window.

## 5.4.3. Managing scan exclusions

If the configured scan exclusions are no longer needed, it is recommended that you delete them or disable scan exclusions.

To manage scan exclusions, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Exclusions** tab. Use the options in the **Files and folders** section to manage scan exclusions.
4. To remove or edit scan exclusions, click one of the available links. Proceed as follows:
  - To remove an entry from the table, select it and click the **Remove** button.
  - To edit an entry from the table, double-click it (or select it and click the **Edit** button). A new window will appear where you can change the extension or the path to be excluded and the type of scanning you want them to be excluded from, as needed. Make the necessary changes, then click **Modify**.
5. To turn off scan exclusions, use the corresponding switch.

## 5.5. Managing quarantined files

Bitdefender isolates the malware-infected files it cannot disinfect and the suspicious files in a secure area named quarantine. When a virus is in quarantine it cannot do any harm because it cannot be executed or read.

By default, quarantined files are automatically sent to Bitdefender Labs in order to be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

In addition, Bitdefender scans the quarantined files after each malware signature update. Cleaned files are automatically moved back to their original location.

To check and manage quarantined files, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Quarantine** tab.
4. Quarantined files are managed automatically by Bitdefender according to the default quarantine settings. Though not recommended, you can adjust the quarantine settings according to your preferences.

### **Rescan quarantine after virus definitions update**

Keep this option turned on to automatically scan quarantined files after each virus definitions update. Cleaned files are automatically moved back to their original location.

### **Send quarantined files to Bitdefender for further analysis**

Keep this option turned on to automatically send quarantined files to Bitdefender Labs. The sample files will be analyzed by the Bitdefender

malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

## **Delete content older than {30} days**

By default, quarantined files older than 30 days are automatically deleted. If you want to change this interval, type a new value in the corresponding field. To disable automatic deletion of old quarantined files, type 0.

5. To delete a quarantined file, select it and click the **Delete** button. If you want to restore a quarantined file to its original location, select it and click **Restore**.

## 5.6. Active Virus Control

Bitdefender Active Virus Control is an innovative proactive detection technology which uses advanced heuristic methods to detect new potential threats in real time.

Active Virus Control continuously monitors the applications running on the computer, looking for malware-like actions. Each of these actions is scored and an overall score is computed for each process. When the overall score for a process reaches a given threshold, the process is considered to be harmful and it is blocked automatically.

If Autopilot is off, you will be notified through a pop-up window about the blocked application. Otherwise, the application will be blocked without any notification. You can check what applications have been detected by Active Virus Control in the **Events** window.

### 5.6.1. Checking detected applications

To check the applications detected by Active Virus Control, follow these steps:

1. Open the Bitdefender window.
2. Click the **Events** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Active Virus Control** tab.
4. Click an event to view details about it.
5. If you trust the application, you can configure Active Virus Control not to block it anymore by clicking **Allow and monitor**. Active Virus Control will continue to monitor excluded applications. If an excluded application is detected to perform suspicious activities, the event will simply be logged and reported to Bitdefender Cloud as detection error.

### 5.6.2. Turning on or off Active Virus Control

To turn on or off Active Virus Control, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.

3. Click **Antivirus** on the left-side menu and then the **Shield** tab.
4. Click the switch to turn on or off Active Virus Control.

## 5.6.3. Adjusting the Active Virus Control protection

If you notice that Active Virus Control detects legitimate applications often, you should set a more permissive protection level.

To adjust the Active Virus Control protection, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Shield** tab.
4. Make sure Active Virus Control is turned on.
5. Drag the slider along the scale to set the desired protection level. Use the description on the right side of the scale to choose the protection level that better fits your security needs.



### Note

As you set the protection level higher, Active Virus Control will require fewer signs of malware-like behavior to report a process. This will lead to a higher number of applications being reported and, at the same time, to an increased likelihood of false positives (clean applications detected as malicious).

## 5.6.4. Managing excluded processes

You can configure exclusion rules for trusted applications so that Active Virus Control does not block them if they perform malware-like actions. Active Virus Control will continue to monitor excluded applications. If an excluded application is detected to perform suspicious activities, the event will simply be logged and reported to Bitdefender Cloud as detection error.

To manage Active Virus Control process exclusions, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Exclusions** tab.
4. Click the **Excluded processes** link. In the window that appears, you can manage the Active Virus Control process exclusions.
5. Add exclusions by following these steps:
  - a. Click the **Add** button, located at the top of the exclusions table.



- b. Click **Browse**, find and select the application you want to be excluded and then click **OK**.
  - c. Keep the **Allow** option selected to prevent Active Virus Control from blocking the application.
  - d. Click **Add**.
6. To remove or edit exclusions, proceed as follows:
- To remove an entry from the table, select it and click the **Remove** button.
  - To edit an entry from the table, double-click it (or select it and click the **Edit** button). Make the necessary changes, then click **Modify**.
7. Click **OK** to save the changes and close the window.

## 5.7. Fixing system vulnerabilities

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

Bitdefender provides two easy ways to fix the vulnerabilities of your system:

- You can scan your system for vulnerabilities and fix them step by step using the **Vulnerability Scan** wizard.
- Using automatic vulnerability monitoring, you can check and fix detected vulnerabilities in the **Events** window.

You should check and fix system vulnerabilities every one or two weeks.

### 5.7.1. Scanning your system for vulnerabilities

To fix system vulnerabilities using the Vulnerability Scan wizard, follow these steps:

1. Open the Bitdefender window.
2. Go to the **Antivirus** panel.
3. Click **Scan now** and then select **Vulnerability Scan**.
4. Follow the six-step guided procedure to remove vulnerabilities from your system. You can navigate through the wizard using the **Next** button. To exit the wizard, click **Cancel**.
  - a. **Protect your PC**  
Select vulnerabilities to check.
  - b. **Check for issues**

Wait for Bitdefender to finish checking your system for vulnerabilities.

## c. **Windows updates**

You can see the list of critical and non-critical Windows updates that are not currently installed on your computer. Select the updates you want to install.

To initiate the installation of selected updates, click **Next**. Please note that it may take a while to install the updates and some of them may require a system restart to complete the installation. If required, restart the system at your earliest convenience.

## d. **Application updates**

If an application is not up to date, click the provided link to download the latest version.

## e. **Weak passwords**

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

Click **Fix** to modify the weak passwords. You can choose between asking the user to change the password at the next logon or changing the password yourself immediately. For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, \$ or @).

## f. **Summary**

This is where you can view the operation result.

## 5.7.2. Using automatic vulnerability monitoring

Bitdefender scans your system for vulnerabilities regularly, in the background, and keeps records of detected issues in the **Events** window.

To check and fix the detected issues, follow these steps:

1. Open the Bitdefender window.
2. Click the **Events** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Vulnerability** tab.
4. You can see detailed information regarding the detected system vulnerabilities. Depending on the issue, to fix a specific vulnerability proceed as follows:
  - If Windows updates are available, click **Update now** to open the Vulnerability Scan wizard and install them.
  - If an application is outdated, click **Update now** to find a link to the vendor web page from where you can install the latest version of that application.
  - If a Windows user account has a weak password, click **Fix password** to force the user to change the password at the next logon or change the password

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

- If the Windows Autorun feature is enabled, click **Disable** to disable it.

To configure the vulnerability monitoring settings, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Vulnerability** tab.
4. Click the switch to turn on or off Automatic Vulnerability Scan.



### Important

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

5. Choose the system vulnerabilities you want to be regularly checked by using the corresponding switches.

### Critical Windows updates

Check if your Windows operating system has the latest critical security updates from Microsoft.

### Regular Windows updates

Check if your Windows operating system has the latest regular security updates from Microsoft.

### Application updates

Check if crucial web-related applications installed on your system are up-to-date. Outdated applications can be exploited by malicious software, making your PC vulnerable to outside attacks.

### Weak passwords

Check whether the passwords of the Windows accounts configured on the system are easy to guess or not. Setting passwords that are hard to guess (strong passwords) makes it very difficult for hackers to break into your system. A strong password includes uppercase and lowercase letters, numbers and special characters (such as #, \$ or @).

### Media autorun

Check the status of the Windows Autorun feature. This feature enables applications to be automatically started from CDs, DVDs, USB drives or other external devices.

Some types of malware use Autorun to spread automatically from removable media to the PC. This is why it is recommended to disable this Windows feature.



## Note

If you turn off monitoring of a specific vulnerability, related issues will no longer be recorded in the Events window.

## 6. Privacy Control

Your private information is a constant target for cyber criminals. As the threats have spread to nearly the entire spectrum of online activities, improperly protected e-mail, instant messaging and web browsing can lead to information leaks that compromise your privacy.

Bitdefender Privacy Control addresses all these threats with a multitude of components.

- **Antiphishing Protection** - offers a comprehensive set of features that protect your entire web browsing experience, including preventing you from disclosing personal information to fraudulent websites disguised as legitimate ones.
- **Data Protection** - helps you make sure that your personal information is not sent from your computer without your consent. It scans the e-mail and instant messages sent from your computer, as well as any data sent via web pages, and blocks any piece of information protected by the Data Protection rules you have created.
- **Chat Encryption** - encrypts your IM conversations to ensure their contents remain between you and your chat partner.

### 6.1. Antiphishing protection

Bitdefender Antiphishing prevents you from disclosing personal information while browsing the Internet by alerting you about potential phishing web pages.

Bitdefender provides real-time antiphishing protection for:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera
- Yahoo! Messenger
- Windows Live (MSN) Messenger

To configure Antiphishing settings, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Privacy Control** on the left-side menu and then the **Antiphishing** tab.

The settings are grouped into two categories.


#### **Toolbar Functions**

Click the switches to turn on or off:

- Showing the **Bitdefender toolbar** in the web browser.

- Search advisor, a component that rates the results of your Google, Bing and Yahoo! searches, as well as links from Facebook and Twitter by placing an icon in front of every result:

-  You should not visit this web page.

-  This web page may contain dangerous content. Exercise caution if you decide to visit it.

-  This is a safe page to visit.

- Scanning SSL web traffic.

More sophisticated attacks might use secure web traffic to mislead their victims. It is therefore recommended to enable SSL scanning.

## Protection for web browsers

Click the switches to turn on or off:

- Protection against fraud.
- Protection against phishing.
- Protection for instant messaging.

You can create a list of web sites that will not be scanned by the Bitdefender Antiphishing engines. The list should contain only web sites you fully trust. For example, add the web sites where you currently shop online.

To configure and manage the antiphishing whitelist, click the **Whitelist** link. A new window will appear.

To add a site to the whitelist, provide its address in the corresponding field and click **Add**.


To remove a web site from the list, select it in the list and click the corresponding **Remove** link.

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

### 6.1.1. Bitdefender protection in the web browser

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

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera

The Bitdefender toolbar is not your typical browser toolbar. The only thing it adds to your browser is a small dragger  at the top of every web page. Click it to see the toolbar.


The Bitdefender toolbar contains the following elements:

## Page Rating

Depending on how Bitdefender classifies the web page you are currently viewing, one of the following ratings is displayed on the left side of the toolbar:

- The message "This page is not safe" appears on a red background - you should leave the web page immediately.
- The message "Caution is advised" appears on an orange background - this web page may contain dangerous content. Exercise caution if you decide to visit it.
- The message "This page is safe" appears on a green background - this is a safe page to visit.

## Sandbox


Click  to launch the browser in a Bitdefender-provided environment, isolating it from the operating system. This prevents browser-based threats from exploiting browser vulnerabilities to gain control of your system. Use Sandbox when visiting web pages you suspect may contain malware.



### Note


Sandbox is not available on computers running Windows XP.

## Settings

Click  to select individual features to turn on or off:

- Antiphishing Filter
- Antimalware Filter
- Search Advisor

## Power Switch

To enable / disable the toolbar features completely, click  on the right side of the toolbar.

## 6.1.2. Bitdefender alerts in the browser

Whenever you try to visit a website classified as unsafe, the website is blocked and a warning page is displayed in your browser.

The page contains information such as the website URL and the detected threat.

You have to decide what to do next. The following options are available:

- Navigate away from the web page.
- Proceed to the web page, despite the warning, by clicking **I understand the risks, take me there anyway**.

- Add the page to the Antiphishing whitelist by clicking **Add to whitelist**. The page will no longer be scanned by Bitdefender Antiphishing engines.

## 6.2. Data Protection

Data protection prevents sensitive data leaks when you are online.

Consider a simple example: you have created a data protection rule that protects your credit card number. If a spyware software somehow manages to install on your computer, it cannot send your credit card number via e-mail, instant messages or web pages. Moreover, your children cannot use it to buy online or reveal it to people they met on the Internet.

To learn more, please refer to these topics:

- *"About data protection"* (p. 58).
- *"Configuring data protection"* (p. 58).
- *"Managing Rules"* (p. 60).

### 6.2.1. About data protection

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

Based on the rules you create, Data Protection scans the web, e-mail and instant messaging traffic leaving your computer for specific character strings (for example, your credit card number). If there is a match, the respective web page, e-mail or instant message is blocked.

You can create rules to protect any piece of information you might consider personal or confidential, from your phone number or e-mail address to your bank account information. Multiuser support is provided so that users logging on to different Windows user accounts can configure and use their own rules. If your Windows account is an administrator account, the rules you create can be configured to also apply when other users of the computer are logged on to their Windows user accounts.

### 6.2.2. Configuring data protection

If you want to use data protection, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Privacy Control** on the left-side menu and then the **Data Protection** tab.
4. Make sure data protection is enabled.



5. Create rules to protect your sensitive data. For more information, please refer to *"Creating data protection rules"* (p. 59).

## Creating data protection rules

To create a rule, click the **Add rule** button and follow the configuration wizard. You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

### 1. Set Rule Type and Data

You must set the following parameters:

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



#### Important

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

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

### 2. Select Traffic Types and Users

a. Select the type of traffic you want Bitdefender to scan.

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

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

b. Specify the users for which the rule applies.

- **Only for me (current user)** - the rule will apply only to your user account.
- **Limited user accounts** - the rule will apply to you and all limited Windows accounts.
- **All users** - the rule will apply to all Windows accounts.

### 3. Describe Rule

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

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

From now on, any attempt to send the specified data (through e-mail, instant messaging or over a web page) will fail. An entry will be displayed in the **Events** window indicating that Bitdefender has blocked identity specific content from being sent.

## 6.2.3. Managing Rules

To manage the data protection rules:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Privacy Control** on the left-side menu and then the **Data Protection** tab.

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

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

To edit a rule select it and click the **Edit rule** button. A new window will appear. Here you can change the name, description and parameters of the rule (type, data and traffic). Click **OK** to save the changes.

## 6.3. Chat Encryption

The contents of your instant messages should remain between you and your chat partner. By encrypting your conversations, you can make sure anyone trying to intercept them on their way to and from your contacts will not be able to read their contents.

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

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



### Important

Bitdefender will not encrypt a conversation if a chat partner uses a web-based chat application such as Meebo, or if one of the chat partners uses Yahoo! and the other Windows Live (MSN).

To configure instant messaging encryption:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Privacy Control** on the left-side menu and then the **Encryption** tab.

By default, Chat Encryption is enabled for both Yahoo Messenger and Windows Live (MSN) Messenger. You can disable Chat Encryption for one or both applications by clicking the corresponding switch.

## 7. Network Map

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

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

1. Enable the Bitdefender network on your computer. Set your computer as **Server computer**.
2. Go to each computer you want to manage and join the network (set the password). Set each computer as **Regular computer**.
3. Go back to your computer and add the computers you want to manage.

### 7.1. Enabling the Bitdefender network

To enable the Bitdefender network, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Network Map** on the left-side menu.
4. Click **Enable Network**. You will be prompted to configure the management password for the network map.
5. Type the same password in each of the edit fields.
6. Set the role of the computer in the Bitdefender network map:
  - **Server computer** - select this option on the computer that will be used to manage all the other ones.
  - **Regular computer** - select this option on the computers that will be managed by the Server Computer.
7. Click **OK**.

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

The **Disable connection** button appears.



#### Note

You can also enable the network map from the main Bitdefender window:

1. Open the Bitdefender window.
2. Go to the **Network Map** panel.
3. Click **Manage** and select **Enable Network** from the drop-down menu.

## 7.2. Adding computers to the Bitdefender network

Any computer will be automatically added to the network if it meets the following criteria:

- the Bitdefender network map was enabled on it.
- the role was set to Regular Computer.
- the password set when enabling the network is the same as the password set on the Server Computer.



### Note

You can scan the network map for computers meeting the criteria at any time by clicking the **Auto discover** button.

To manually add a computer to the Bitdefender network map from the Server Computer, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Network Map** on the left-side menu.
4. Click **Add Computer**.
5. Type the management password and click **OK**. A new window will appear.

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



Indicates an online computer with no Bitdefender products installed.



Indicates an online computer with Bitdefender installed.



Indicates an offline computer with Bitdefender installed.

6. Do one of the following:
  - Select from the list the name of the computer to add.
  - Type the IP address or the name of the computer to add in the corresponding field.
7. Click **Add**.
8. Type the management password configured on the respective computer.
9. Click **OK**. If you have provided the correct password, the selected computer name will appear in the network map.

## 7.3. Managing the Bitdefender network

Once you have successfully created a Bitdefender network map, you can manage all Bitdefender products from the Server Computer.

To run several tasks on all managed computers, follow these steps:

1. Open the Bitdefender window.
2. Go to the **Network Map** panel.
3. Click **Manage** and select the corresponding buttons from the drop-down menu:
  - **Disable connection** - allows you to disable the network.
  - **Scan All** - allows you to scan all managed computers at the same time.
  - **Update All** allows you to update all managed computers at the same time.

Before running a task on a specific computer, you will be prompted to provide the local management password. Type the management password and click **OK**.

To see the entire Network Map and access all management tasks, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Network Map** on the left-side menu.

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

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

### **Register product**

Allows you to register Bitdefender on this computer by entering a license key.

### **Configure password for product settings**

Allows you to create a password to restrict access to Bitdefender settings on this PC.

### **Run an on-demand scan task**

Allows you to run an on-demand scan on the remote computer. You can perform any of the following scan tasks: Quick Scan or Full System Scan.

### **Fix all issues**

Allows you to fix the issues that are affecting the security of this computer by following the **Fix All Issues** wizard.

### **View events**

Allows you access to the **Events** module of the Bitdefender product installed on this computer.

### **Update Now**

Initiates the Update process for the Bitdefender product installed on this computer.

## Set as Update Server of this network

Allows you to set this computer as update server for all Bitdefender products installed on the computers in this network. Using this option will reduce internet traffic, because only one computer in the network will connect to the internet to download updates.

## Remove PC from network map

Allows you to remove a PC from the network.



### Note

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

## 8. Update

New malware is found and identified every day. This is why it is very important to keep Bitdefender up to date with the latest malware signatures.

If you are connected to the Internet through broadband or DSL, Bitdefender takes care of this itself. By default, it checks for updates when you turn on your computer and every **hour** after that. If an update is detected, it is automatically downloaded and installed on your computer.

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



### Important

To be protected against the latest threats keep Automatic Update turned on.

In some particular situations, your intervention is required in order to keep your Bitdefender protection up-to-date:

- If your computer connects to the Internet through a proxy server, you must configure the proxy settings as described in *"How do I configure Bitdefender to use a proxy Internet connection?"* (p. 30).
- If you do not have Internet connection, you can update Bitdefender manually as described in *"My computer is not connected to the Internet. How do I update Bitdefender?"* (p. 74). The manual update file is released once a week.
- Errors may occur while downloading updates on a slow Internet connection. To find out how to overcome such errors, please refer to *"How to update Bitdefender on a slow Internet connection"* (p. 73).
- If you are connected to the Internet through a dial-up connection, then it is recommended to regularly update Bitdefender by user request. For more information, please refer to *"Performing an update"* (p. 67).

### 8.1. Checking if Bitdefender is up-to-date

To check if your Bitdefender protection is up-to-date, follow these steps:

1. Open the Bitdefender window.
2. Go to the **Update** panel.
3. The time of the last update is displayed just under the panel's name.

For detailed information about the latest updates, check the update events:

1. In the main window, click **Events** on the upper toolbar.
2. Click **Update** on the left-side menu.




You can find out when updates were initiated and information about them (whether they were successful or not, if they require a restart to complete the installation). If required, restart the system at your earliest convenience.

## 8.2. Performing an update

In order to perform updates, an Internet connection is required.

To start an update, do any of the following:

- Open the Bitdefender window, go to the **Update** panel and click **Update now**.
- Right-click the Bitdefender icon  in the **system tray** and select **Update now**.

The Update module will connect to the Bitdefender update server and it will check for updates. If an update is detected, you will be asked to confirm it or the update will be performed automatically, depending on the **update settings**.



### Important

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

## 8.3. Turning on or off automatic update

To turn on or off automatic update, follow these steps:

1. Open the Bitdefender window.
2. Go to the **Update** panel.
3. Click the switch to turn on or off Automatic Update.
4. If you want to turn off automatic update, a warning window will appear. You must confirm your choice by selecting from the menu how long you want the automatic update to be disabled. You can disable the automatic update for 5, 15 or 30 minutes, for an hour, permanently or until the system restart.



### Warning

This is a critical security issue. We recommend you to disable automatic update for as little time as possible. If Bitdefender is not updated regularly, it will not be able to protect you against the latest threats.

## 8.4. Adjusting update settings

The updates can be performed from the local network, over the Internet, directly or through a proxy server. By default, Bitdefender will check for updates every hour, over the Internet, and install the available updates without alerting you.

The default update settings are suited for most users and you do not normally need to change them.

To adjust the update settings, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Update** on the left-side menu.
4. Adjust the settings according to your preferences.

## Update location

Bitdefender is configured to update from the Bitdefender update servers on the Internet. The update location is `http://upgrade.bitdefender.com`, a generic Internet address that is automatically redirected to the closest Bitdefender update server in your region.

Do not change the update location unless advised by a Bitdefender representative or by your network administrator (if you are connected to an office network).

If you have installed Bitdefender on several computers in your household, you can set up a Bitdefender home network and then designate one of your computers as update server. Detailed information is provided in "*Network Map*" (p. 62). The Bitdefender program installed on the designated update server will update from the Internet. The Bitdefender programs on the other computers will get their updates from the local update server (their update location is changed accordingly automatically). This configuration is intended to minimize Internet traffic and to optimize updates.

You can switch back to the generic Internet update location by clicking **Default**.

## Update processing rules

You can choose between three ways to download and install updates:

- **Silent update** - Bitdefender automatically downloads and implements the update.
- **Prompt before downloading** - every time an update is available, you will be prompted before downloading it.
- **Prompt before installing** - every time an update was downloaded, you will be prompted before installing it.

Some updates require a restart to complete the installation. By default, if an update requires a restart, Bitdefender will keep working with the old files until the user voluntarily restarts the computer. This is to prevent the Bitdefender update process from interfering with the user's work.

If you want to be prompted when an update requires a restart, turn off the **Postpone reboot** option by clicking the corresponding switch.

## P2P updates

Besides the normal update mechanism, Bitdefender also uses a smart update sharing system based on a peer-to-peer (P2P) protocol to distribute malware signature updates between Bitdefender users.

You can turn on or off the P2P update options using the corresponding switches.

### **Use P2P update system**

Turn on this option to download malware signature updates from other Bitdefender users using the P2P update system. Bitdefender uses ports 8880 - 8889 for peer-to-peer update.

### **Distribute Bitdefender files**

Turn on this option to share the latest malware signatures available on your computer with other Bitdefender users.

## 9. Safego protection for social networks

You trust your online friends. But do you trust their computers? Use Safego protection for social networks to protect your account and your friends from online threats.

Safego is a Facebook application developed by Bitdefender to keep your social networking account safe. Its role is to scan the links you receive from your Facebook friends and monitor your account privacy settings.



### Note

A MyBitdefender account is required in order to use this feature.  
For more information, please refer to "*Product registration*" (p. 7).

These are its main features:

- automatically scans the posts in your News Feed for malicious links.
- protects your account against online threats.

When it detects a post or a comment which is a spam, a phishing or a malware, you will receive a warning message.

- warns your friends on suspicious links posted on their News Feed.
- helps you build a safe network of friends using the **Friend'O'Meter** feature.
- get a system safety status check provided by Bitdefender QuickScan.

To access Safego from your Bitdefender product, follow these steps:

1. Open the Bitdefender window.
2. Go to the **Safego** panel.
3. Click **Activate**. You will be directed to your account.

If you already activated Safego, you will be able to access statistics regarding its activity by clicking the **View Reports** button.

4. Use your Facebook login information to connect to the Safego application.
5. Allow Safego access to your Facebook account.

## 10. Troubleshooting

This chapter presents some problems you may encounter when using Bitdefender and provides you with possible solutions to these problems. Most of these problems can be solved through the appropriate configuration of the product settings.

- *“My system appears to be slow”* (p. 71)
- *“Scan doesn't start”* (p. 72)
- *“I can no longer use an application”* (p. 72)
- *“How to update Bitdefender on a slow Internet connection”* (p. 73)
- *“My computer is not connected to the Internet. How do I update Bitdefender?”* (p. 74)
- *“Bitdefender services are not responding”* (p. 74)
- *“Bitdefender removal failed”* (p. 75)
- *“My system doesn't boot up after installing Bitdefender”* (p. 75)

If you cannot find your problem here, or if the presented solutions do not solve it, you can contact the Bitdefender technical support representatives as presented in chapter *“Support”* (p. 85).

### 10.1. My system appears to be slow

Usually, after installing a security software, there may appear a slight slowdown of the system, which to a certain degree is normal.

If you notice a significant slow down, this issue can appear for the following reasons:

- **Bitdefender is not the only security program installed on the system.**  
Though Bitdefender searches and removes the security programs found during the installation, it is recommended to remove any other antivirus program you may use before installing Bitdefender. For more information, please refer to *“How do I remove other security solutions?”* (p. 91).
- **The Minimum System Requirements for running Bitdefender are not met.**  
If your machine does not meet the Minimum System Requirements, the computer will become sluggish, especially when multiple applications are running at the same time. For more information, please refer to *“Minimum system requirements”* (p. 1).
- **Your hard disk drives are too fragmented.**  
File fragmentation slows down file access and decreases system performance.

To defragment your disk using your Windows operating system, follow the path from the Windows start menu: **Start** → **All Programs** → **Accessories** → **System Tools** → **Disk Defragmenter**.

## 10.2. Scan doesn't start

This type of issue can have two main causes:

- **A previous Bitdefender installation which was not completely removed or a faulty Bitdefender installation.**

In this case, follow these steps:

1. Remove Bitdefender completely from the system:
  - a. Go to <http://www.bitdefender.com/uninstall> and download the uninstall tool on your computer.
  - b. Run the uninstall tool using administrator privileges.
  - c. Restart your computer.
2. Reinstall Bitdefender on the system.

- **Bitdefender is not the only security solution installed on your system.**

In this case, follow these steps:

1. Remove the other security solution. For more information, please refer to "*How do I remove other security solutions?*" (p. 91).
2. Remove Bitdefender completely from the system:
  - a. Go to <http://www.bitdefender.com/uninstall> and download the uninstall tool on your computer.
  - b. Run the uninstall tool using administrator privileges.
  - c. Restart your computer.
3. Reinstall Bitdefender on the system.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 86).

## 10.3. I can no longer use an application

This issue occurs when you are trying to use a program which was working normally before installing Bitdefender.

You may encounter one of these situations:

- You could receive a message from Bitdefender that the program is trying to make a modification to the system.
- You could receive an error message from the program you're trying to use.

This type of situation occurs when the Active Virus Control module mistakenly detects some applications as malicious.

Active Virus Control is a Bitdefender module which constantly monitors the applications running on your system and reports those with potentially malicious behavior. Since this feature is based on a heuristic system, there may be cases when legitimate applications are reported by Active Virus Control.

When this situation occurs, you can exclude the respective application from being monitored by Active Virus Control.

To add the program to the exclusions list, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Antivirus** on the left-side menu and then the **Exclusions** tab.
4. Click the **Excluded Processes** link. In the window that appears, you can manage the Active Virus Control process exclusions.
5. Add exclusions by following these steps:
  - a. Click the **Add** button, located at the top of the exclusions table.
  - b. Click **Browse**, find and select the application you want to be excluded and then click **OK**.
  - c. Keep the **Allow** option selected to prevent Active Virus Control from blocking the application.
  - d. Click **Add**.

If this information was not helpful, you can contact Bitdefender for support as described in section *"Asking for help"* (p. 86).

## 10.4. How to update Bitdefender on a slow Internet connection

If you have a slow Internet connection (such as dial-up), errors may occur during the update process.

To keep your system up to date with the latest Bitdefender malware signatures, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. Click **Update** on the left-side menu and then the **Update** tab.
4. Under **Update processing rules**, select **Prompt before downloading**.
5. Click the **Home** button on the upper toolbar.
6. Go to the **Update** panel and click **Update now**.

7. Select only **Signatures updates** and then click **Ok**.
8. Bitdefender will download and install only the malware signature updates.

## 10.5. My computer is not connected to the Internet. How do I update Bitdefender?

If your computer is not connected to the Internet, you must download the updates manually to a computer with Internet access and then transfer them to your computer using a removable device, such as a flash drive.

Follow these steps:

1. On a computer with Internet access, open a web browser and go to:  
<http://www.bitdefender.com/site/view/Desktop-Products-Updates.html>
2. In the **Manual Update** column, click the link corresponding to your product and system architecture. If you do not know whether your Windows is running on 32 or 64 bits, please refer to *"Am I using a 32 bit or a 64 bit version of Windows?"* (p. 92).
3. Save the file named `weekly.exe` to the system.
4. Transfer the downloaded file on a removable device, such as a flash drive, and then to your computer.
5. Double-click the file and follow the wizard steps.

## 10.6. Bitdefender services are not responding

This article helps you troubleshoot the **Bitdefender Services are not responding** error. You may encounter this error as follows:

- The Bitdefender icon in the **system tray** is grayed out and you are informed that the Bitdefender services are not responding.
- The Bitdefender window indicates that the Bitdefender services are not responding.

The error may be caused by one of the following conditions:

- an important update is being installed.
- temporary communication errors between the Bitdefender services.
- some of the Bitdefender services are stopped.
- other security solutions running on your computer at the same time with Bitdefender.

To troubleshoot this error, try these solutions:

1. Wait a few moments and see if anything changes. The error may be temporary.



2. Restart the computer and wait a few moments until Bitdefender is loaded. Open Bitdefender to see if the error persists. Restarting the computer usually solves the problem.
3. Check if you have any other security solution installed as they may disrupt the normal operation of Bitdefender. If this is the case, we recommend you to remove all of the other security solutions and then reinstall Bitdefender.

For more information, please refer to *"How do I remove other security solutions?"* (p. 91).

If the error persists, please contact our support representatives for help as described in section *"Asking for help"* (p. 86).

## 10.7. Bitdefender removal failed

This article helps you troubleshoot errors that may occur when removing Bitdefender. There are two possible situations:

- During removal, an error screen appears. The screen provides a button to run an uninstall tool that will clean up the system.
- The removal hangs out and, possibly, your system freezes. Click **Cancel** to abort the removal. If this does not work, restart the system.

If removal fails, some Bitdefender registry keys and files may remain in your system. Such remainders may prevent a new installation of Bitdefender. They may also affect system performance and stability.

In order to completely remove Bitdefender from your system, follow these steps:

1. Go to <http://www.bitdefender.com/uninstall> and download the uninstall tool on your computer.
2. Run the uninstall tool using administrator privileges.
3. Restart your computer.

If this information was not helpful, you can contact Bitdefender for support as described in section *"Asking for help"* (p. 86).

## 10.8. My system doesn't boot up after installing Bitdefender

If you just installed Bitdefender and cannot reboot your system in normal mode anymore there may be various reasons for this issue.

Most probably this is caused by a previous Bitdefender installation which was not removed properly or by another security solution still present on the system.

This is how you may address each situation:

- **You had Bitdefender before and you did not remove it properly.**

To solve this, follow these steps:

1. Reboot your system and enter in Safe Mode. To find out how to do this, please refer to *"How do I restart in Safe Mode?"* (p. 92).
2. Remove Bitdefender from your system:
  - a. Go to <http://www.bitdefender.com/uninstall> and download the uninstall tool on your computer.
  - b. Run the uninstall tool using administrator privileges.
  - c. Restart your computer.
3. Reboot your system in normal mode and reinstall Bitdefender.

● **You had a different security solution before and you did not remove it properly.**

To solve this, follow these steps:

1. Reboot your system and enter in Safe Mode. To find out how to do this, please refer to *"How do I restart in Safe Mode?"* (p. 92).
2. Remove Bitdefender from your system:
  - a. Go to <http://www.bitdefender.com/uninstall> and download the uninstall tool on your computer.
  - b. Run the uninstall tool using administrator privileges.
  - c. Restart your computer.
3. In order to correctly uninstall the other software, go to their website and run their uninstall tool or contact them directly in order to provide you with the uninstall guidelines.
4. Reboot your system in normal mode and reinstall Bitdefender.

**You have already followed the steps above and the situation is not solved.**

To solve this, follow these steps:

1. Reboot your system and enter in Safe Mode. To find out how to do this, please refer to *"How do I restart in Safe Mode?"* (p. 92).
2. Use the System Restore option from Windows to restore the computer to an earlier date before installing the Bitdefender product. To find out how to do this, please refer to *"How do I use System Restore in Windows?"* (p. 93).
3. Reboot the system in normal mode and contact our support representatives for help as described in section *"Asking for help"* (p. 86).

## 11. Removing malware from your system

Malware can affect your system in many different ways and the Bitdefender approach depends on the type of malware attack. Because viruses change their behavior frequently, it is difficult to establish a pattern for their behavior and their actions.

There are situations when Bitdefender cannot automatically remove the malware infection from your system. In such cases, your intervention is required.

- *"Bitdefender Rescue Mode" (p. 77)*
- *"What to do when Bitdefender finds viruses on your computer?" (p. 79)*
- *"How do I clean a virus in an archive?" (p. 80)*
- *"How do I clean a virus in an e-mail archive?" (p. 81)*
- *"What to do if I suspect a file as being dangerous?" (p. 82)*
- *"How to clean the infected files from System Volume Information" (p. 82)*
- *"What are the password-protected files in the scan log?" (p. 83)*
- *"What are the skipped items in the scan log?" (p. 84)*
- *"What are the over-compressed files in the scan log?" (p. 84)*
- *"Why did Bitdefender automatically delete an infected file?" (p. 84)*

If you cannot find your problem here, or if the presented solutions do not solve it, you can contact the Bitdefender technical support representatives as presented in chapter *"Support" (p. 85)*.

### 11.1. Bitdefender Rescue Mode

**Rescue Mode** is a Bitdefender feature that allows you to scan and disinfect all existing hard drive partitions outside of your operating system.

Once Bitdefender Antivirus Plus 2012 is installed, Rescue Mode can be used even if you are no longer able to boot into Windows.

#### Starting your system in Rescue Mode

You can enter Rescue Mode in one of two ways:

From the Bitdefender window

To enter Rescue Mode directly from Bitdefender, follow these steps:

1. Go to the **Antivirus** panel.
2. Click **Scan Now** and select **Rescue Mode** from the drop-down menu.

A confirmation window will appear. Click **Yes** to reboot your computer.

3. After the computer restarts, a menu will appear prompting you to select an operating system. Choose **Bitdefender Rescue Image** and press the **Enter** key to boot into a Bitdefender environment from where you can clean up your Windows partition.
4. If prompted, press **Enter** and select the screen resolution closest to the one you normally use. Then press **Enter** again.

Bitdefender Rescue Mode will load in a few moments.

Boot your computer directly into Rescue Mode

If Windows no longer starts, you can boot your computer directly into Bitdefender Rescue Mode by following the steps below.



## Note

This method is not available on computers running Windows XP.

1. Start / reboot your computer and start pressing the **space** key on your keyboard before the Windows logo appears.
2. A menu will appear prompting you to select an operating system to start. Press **TAB** to go to the tools area. Choose **Bitdefender Rescue Image** and press the **Enter** key to boot into a Bitdefender environment from where you can clean up your Windows partition.
3. If prompted, press **Enter** and select the screen resolution closest to the one you normally use. Then press **Enter** again.

Bitdefender Rescue Mode will load in a few moments.

## Scanning your system in Rescue Mode

To scan your system in Rescue Mode, follow these steps:

1. Enter Rescue Mode, as described in [“Starting your system in Rescue Mode”](#) (p. 77).
2. The Bitdefender logo will appear and the antivirus engines will start to be copied.
3. A welcome window will then appear. Click **Continue**.
4. An update of the antivirus signatures is started.
5. After the update is completed, the Bitdefender On-demand Antivirus Scanner window will appear.
6. Click **Scan Now**, select the scan target in the window that appears and click **Open** to start scanning.

It is recommended to scan your entire Windows partition.



## Note

When working in Rescue Mode, you are dealing with Linux-type partition names. Disk partitions will appear as `sda1` probably corresponding to the (C:) Windows-type partition, `sda2` corresponding to (D:) and so on.

7. Wait for the scan to complete. If any malware is detected, follow the instructions to remove the threat.
8. To exit Rescue Mode, right-click in an empty area of the Desktop, select **Logout** in the menu that appears and then choose whether to reboot or shut down the computer.

## 11.2. What to do when Bitdefender finds viruses on your computer?

You may find out there is a virus on your computer in one of these ways:

- You scanned your computer and Bitdefender found infected items on it.
- A virus alert informs you that Bitdefender blocked one or multiple viruses on your computer.

In such situations, update Bitdefender to make sure you have the latest malware signatures and run a Full System Scan to analyze the system.

As soon as the full scan is over, select the desired action for the infected items (Disinfect, Delete, Move to quarantine).



## Warning

If you suspect the file is part of the Windows operating system or that it is not an infected file, do not follow these steps and contact Bitdefender Customer Care as soon as possible.

If the selected action could not be taken and the scan log reveals an infection which could not be deleted, you have to remove the file(s) manually:

### The first method can be used in normal mode:

1. Turn off the Bitdefender real-time antivirus protection:
  - a. Open the Bitdefender window.
  - b. Click the **Settings** button in the upper toolbar.
  - c. Click **Antivirus** on the left-side menu and then the **Shield** tab.
  - d. Click the switch to turn off **on-access scanning**.
2. Display hidden objects in Windows. To find out how to do this, please refer to *"How do I display hidden objects in Windows?"* (p. 93).

3. Browse to the location of the infected file (check the scan log) and delete it.
4. Turn on the Bitdefender real-time antivirus protection.

**In case the first method failed to remove the infection, follow these steps:**

1. Reboot your system and enter in Safe Mode. To find out how to do this, please refer to *"How do I restart in Safe Mode?"* (p. 92).
2. Display hidden objects in Windows.
3. Browse to the location of the infected file (check the scan log) and delete it.
4. Reboot your system and enter in normal mode.

If this information was not helpful, you can contact Bitdefender for support as described in section *"Asking for help"* (p. 86).

## 11.3. How do I clean a virus in an archive?

An archive is a file or a collection of files compressed under a special format to reduce the space on disk necessary for storing the files.

Some of these formats are open formats, thus providing Bitdefender the option to scan inside them and then take appropriate actions to remove them.

Other archive formats are partially or fully closed, and Bitdefender can only detect the presence of viruses inside them, but is not able to take any other actions.

If Bitdefender notifies you that a virus has been detected inside an archive and no action is available, it means that removing the virus is not possible due to restrictions on the archive's permission settings.

Here is how you can clean a virus stored in an archive:

1. Identify the archive that includes the virus by performing a Full System Scan of the system.
2. Turn off the Bitdefender real-time antivirus protection:
  - a. Open the Bitdefender window.
  - b. Click the **Settings** button in the upper toolbar.
  - c. Click **Antivirus** on the left-side menu and then the **Shield** tab.
  - d. Click the switch to turn off **on-access scanning**.
3. Go to the location of the archive and decompress it using an archiving application, like WinZip.
4. Identify the infected file and delete it.
5. Delete the original archive in order to make sure the infection is totally removed.
6. Recompress the files in a new archive using an archiving application, like WinZip.

7. Turn on the Bitdefender real-time antivirus protection and run a Full system scan in order to make sure there is no other infection on the system.



## Note

It's important to note that a virus stored in an archive is not an immediate threat to your system, since the virus has to be decompressed and executed in order to infect your system.

If this information was not helpful, you can contact Bitdefender for support as described in section *"Asking for help"* (p. 86).

## 11.4. How do I clean a virus in an e-mail archive?

Bitdefender can also identify viruses in e-mail databases and e-mail archives stored on disk.

Sometimes it is necessary to identify the infected message using the information provided in the scan report, and delete it manually.

Here is how you can clean a virus stored in an e-mail archive:

1. Scan the e-mail database with Bitdefender.
2. Turn off the Bitdefender real-time antivirus protection:
  - a. Open the Bitdefender window.
  - b. Click the **Settings** button in the upper toolbar.
  - c. Click **Antivirus** on the left-side menu and then the **Shield** tab.
  - d. Click the switch to turn off **on-access scanning**.
3. Open the scan report and use the identification information (Subject, From, To) of the infected messages to locate them in the e-mail client.
4. Delete the infected messages. Most e-mail clients also move the deleted message to a recovery folder, from which it can be recovered. You should make sure the message is deleted also from this recovery folder.
5. Compact the folder storing the infected message.
  - In Outlook Express: On the File menu, click Folder, then Compact All Folders.
  - In Microsoft Outlook: On the File menu, click Data File Management. Select the personal folders (.pst) files you intend to compact, and click Settings. Click Compact.
6. Turn on the Bitdefender real-time antivirus protection.

If this information was not helpful, you can contact Bitdefender for support as described in section *"Asking for help"* (p. 86).

## 11.5. What to do if I suspect a file as being dangerous?

You may suspect a file from your system as being dangerous, even though your Bitdefender product did not detect it.

To make sure your system is protected, follow these steps:

1. Run a **Full System Scan** with Bitdefender. To find out how to do this, please refer to *"How do I scan my system?"* (p. 28).
2. If the scan result appears to be clean, but you still have doubts and want to make sure about the file, contact our support representatives so that we may help you.

To find out how to do this, please refer to *"Asking for help"* (p. 86).

## 11.6. How to clean the infected files from System Volume Information

The System Volume Information folder is a zone on your hard drive created by the Operating System and used by Windows for storing critical information related to the system configuration.

The Bitdefender engines can detect any infected files stored by the System Volume Information, but being a protected area it may not be able to remove them.

The infected files detected in the System Restore folders will appear in the scan log as follows:

```
?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-...
```

To completely and immediately remove the infected file or files in the data store, disable and re-enable the System Restore feature.

When System Restore is turned off, all the restore points are removed.

When System Restore is turned on again, new restore points are created as the schedule and events require.

In order to disable the System Restore follow these steps:

### ● For Windows XP:

1. Follow this path: **Start** → **All Programs** → **Accessories** → **System Tool** → **System Restore**
2. Click **System Restore Settings** located on the left hand side of the window.
3. Select the **Turn off System Restore** check box on all drives, and click **Apply**.
4. When you are warned that all existing Restore Points will be deleted, click **Yes** to continue.
5. To turn on the System Restore, clear the **Turn off System Restore** check box on all drives, and click **Apply**.



## ● For Windows Vista:

1. Follow this path: **Start** → **Control Panel** → **System and Maintenance** → **System**
2. In the left pane, click **System Protection**.  
If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
3. To turn off the System Restore clear the check boxes corresponding to each drive and click **Ok**.
4. To turn on the System Restore select the check boxes corresponding to each drive and click **Ok**.

## ● For Windows 7:

1. Click **Start**, right-click **Computer** and click **Properties**.
2. Click **System protection** link in the left pane.
3. In the **System protection** options, select each drive letter and click **Configure**.
4. Select **Turn off system protection** and click **Apply**.
5. Click **Delete**, click **Continue** when prompted and then click **Ok**.

If this information was not helpful, you can contact Bitdefender for support as described in section *"Asking for help"* (p. 86).

## 11.7. What are the password-protected files in the scan log?

This is only a notification which indicates that Bitdefender has detected these files are either protected with a password or by some form of encryption.

Most commonly, the password-protected items are:

- Files that belong to another security solution.
- Files that belong to the operating system.

In order to actually scan the contents, these files would need to either be extracted or otherwise decrypted.

Should those contents be extracted, Bitdefender's real-time scanner would automatically scan them to keep your computer protected. If you want to scan those files with Bitdefender, you have to contact the product manufacturer in order to provide you with more details on those files.

Our recommendation to you is to ignore those files because they are not a threat for your system.

## 11.8. What are the skipped items in the scan log?

All files that appear as Skipped in the scan report are clean.

For increased performance, Bitdefender does not scan files that have not changed since the last scan.

## 11.9. What are the over-compressed files in the scan log?

The over-compressed items are elements which could not be extracted by the scanning engine or elements for which the decryption time would have taken too long making the system unstable.

Overcompressed means that Bitdefender skipped scanning within that archive because unpacking it proved to take up too many system resources. The content will be scanned on real time access if needed.

## 11.10. Why did Bitdefender automatically delete an infected file?

If an infected file is detected, Bitdefender will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

This is usually the case with installation files that are downloaded from untrustworthy websites. If you find yourself in such a situation, download the installation file from the manufacturer's website or other trusted website.

## 12. Getting help

### 12.1. Support

Bitdefender strives to provide its customers with an unparalleled level of fast and accurate support. If you experience any issue with or if you have any question about your Bitdefender product, you can use several online resources to quickly find a solution or an answer. Or, if you prefer, you can contact the Bitdefender Customer Care team. Our support representatives will answer your questions in a timely manner and they will provide you with the assistance you need.

#### 12.1.1. Online resources

Several online resources are available to help you solve your Bitdefender-related problems and questions.

- Bitdefender Support Center: <http://www.bitdefender.com/help>
- Bitdefender Support Forum: <http://forum.bitdefender.com>
- the Malware City computer security portal: <http://www.malwarecity.com>

You can also use your favorite search engine to find out more information about computer security, the Bitdefender products and the company.

#### Bitdefender Support Center

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

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

The Bitdefender Support Center is available any time at <http://www.bitdefender.com/help>.

#### Bitdefender Support Forum

The Bitdefender Support Forum provides Bitdefender users with an easy way to get help and to help others.

If your Bitdefender product does not operate well, if it cannot remove specific viruses from your computer or if you have questions about the way it works, post your problem or question on the forum.

Bitdefender support technicians monitor the forum for new posts in order to assist you. You may also get an answer or a solution from a more experienced Bitdefender user.

Before posting your problem or question, please search the forum for a similar or related topic.

The Bitdefender Support Forum is available at <http://forum.bitdefender.com>, in 5 different languages: English, German, French, Spanish and Romanian. Click the **Home & Home Office Protection** link to access the section dedicated to consumer products.

## Malware City Portal

The Malware City portal is a rich source of computer security information. Here you can learn about the various threats your computer is exposed to when connected to the Internet (malware, phishing, spam, cyber-criminals). A useful dictionary helps you understand the computer security terms that you are not familiar with.

New articles are posted regularly to keep you up-to-date with the latest threats discovered, the current security trends and other information on the computer security industry.

The Malware City web page is <http://www.malwarecity.com>.

## 12.1.2. Asking for help

The **Troubleshooting** section provides you with the necessary information regarding the most frequent issues you may encounter when using this product.

If you do not find the solution to your problem in the provided resources, you can contact us directly:

- [“Contact us directly from your Bitdefender product” \(p. 86\)](#)
- [“Contact us through our online Support Center” \(p. 87\)](#)



### Important

To contact the Bitdefender Customer Care you must register your Bitdefender product. For more information, please refer to [“Product registration” \(p. 7\)](#).

## Contact us directly from your Bitdefender product

If you have a working Internet connection, you can contact Bitdefender for assistance directly from the product interface.

Follow these steps:

1. Open the Bitdefender window.
2. Click the **Help and Support** link, located at the bottom-right corner of the window.
3. You have the following options:
  - Read the relevant articles or documents and try the proposed solutions.
  - Launch a search in our database for the information you seek.
  - Use the **Contact support** button to launch the Support Tool and contact the Customer Care Department. You can navigate through the wizard using the **Next** button. To exit the wizard, click **Cancel**.
    - a. Select the agreement check box and click **Next**.
    - b. Complete the submission form with the necessary data:
      - i. Enter your e-mail address.
      - ii. Enter your full name.
      - iii. Choose your country from the corresponding menu.
      - iv. Enter a description of the issue you encountered.
    - c. Please wait for a few minutes while Bitdefender gathers product related information. This information will help our engineers find a solution to your problem.
    - d. Click **Finish** to send the information to the Bitdefender Customer Care Department. You will be contacted as soon as possible.

## Contact us through our online Support Center

If you cannot access the necessary information using the Bitdefender product, please refer to our online Support Center:

1. Go to <http://www.bitdefender.com/help>. The Bitdefender Support Center hosts numerous articles that contain solutions to Bitdefender-related issues.
2. Select your product from the left side column and search the Bitdefender Support Center for articles that may provide a solution to your problem.
3. Read the relevant articles or documents and try the proposed solutions.
4. If the solution does not solve your problem, use the link in the article to contact Bitdefender Customer Care.
5. Contact the Bitdefender support representatives by e-mail, chat or phone.

## 12.2. Contact information

Efficient communication is the key to a successful business. During the past 10 years BITDEFENDER has established an unquestionable reputation by constantly striving for better communication so as to exceed the expectations of our clients and partners. Should you have any questions, do not hesitate to contact us.

### 12.2.1. Web addresses

Sales department: [sales@bitdefender.com](mailto:sales@bitdefender.com)  
Support Center: <http://www.bitdefender.com/help>  
Documentation: [documentation@bitdefender.com](mailto:documentation@bitdefender.com)  
Local distributors: <http://www.bitdefender.com/partners>  
Partner program: [partners@bitdefender.com](mailto:partners@bitdefender.com)  
Media relations: [pr@bitdefender.com](mailto:pr@bitdefender.com)  
Careers: [jobs@bitdefender.com](mailto:jobs@bitdefender.com)  
Virus submissions: [virus\\_submission@bitdefender.com](mailto:virus_submission@bitdefender.com)  
Spam submissions: [spam\\_submission@bitdefender.com](mailto:spam_submission@bitdefender.com)  
Report abuse: [abuse@bitdefender.com](mailto:abuse@bitdefender.com)  
Web site: <http://www.bitdefender.com>

### 12.2.2. Local distributors

The Bitdefender local distributors are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters.

To find a Bitdefender distributor in your country:

1. Go to <http://www.bitdefender.com/site/Partnership/list/>.
2. The contact information of the Bitdefender local distributors should be displayed automatically. If this does not happen, select the country you reside in to view the information.
3. If you do not find a Bitdefender distributor in your country, feel free to contact us by e-mail at [sales@bitdefender.com](mailto:sales@bitdefender.com). Please write your e-mail in English in order for us to be able to assist you promptly.

### 12.2.3. Bitdefender offices

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

#### U.S.A

**Bitdefender, LLC**  
PO Box 667588

# Bitdefender Antivirus Plus 2012

Pompano Beach, FL 33066  
Phone (office&sales): 1-954-776-6262  
Sales: [sales@bitdefender.com](mailto:sales@bitdefender.com)  
Technical support: <http://www.bitdefender.com/help>  
Web: <http://www.bitdefender.com>

## UK and Ireland

Genesis Centre Innovation Way  
Stoke-on-Trent, Staffordshire  
ST6 4BF  
E-mail: [info@bitdefender.co.uk](mailto:info@bitdefender.co.uk)  
Phone: +44 (0) 8451-305096  
Sales: [sales@bitdefender.co.uk](mailto:sales@bitdefender.co.uk)  
Technical support: <http://www.bitdefender.com/help>  
Web: <http://www.bitdefender.co.uk>

## Germany

**Bitdefender GmbH**  
Airport Office Center  
Robert-Bosch-Straße 2  
59439 Holzwickedede  
Deutschland  
Office: +49 2301 91 84 0  
Sales: [vertrieb@bitdefender.de](mailto:vertrieb@bitdefender.de)  
Technical support: <http://kb.bitdefender.de>  
Web: <http://www.bitdefender.de>

## Spain

**Bitdefender España, S.L.U.**  
Avda. Diagonal, 357, 1º 1ª  
08037 Barcelona  
Fax: +34 93 217 91 28  
Phone: +34 902 19 07 65  
Sales: [comercial@bitdefender.es](mailto:comercial@bitdefender.es)  
Technical support: <http://www.bitdefender.es/ayuda>  
Website: <http://www.bitdefender.es>

## Romania

**BITDEFENDER SRL**  
West Gate Park, Building H2, 24 Preciziei Street  
Bucharest  
Fax: +40 21 2641799

# Bitdefender Antivirus Plus 2012

Sales phone: +40 21 2063470

Sales e-mail: [sales@bitdefender.ro](mailto:sales@bitdefender.ro)

Technical support: <http://www.bitdefender.ro/suport>

Website: <http://www.bitdefender.ro>



## 13. Useful information

This chapter presents some important procedures that you must be aware before starting to troubleshoot a technical issue.

Troubleshooting a technical situation in Bitdefender requires a few Windows insights, therefore the next steps are mostly related to the Windows operating system.

- *“How do I remove other security solutions?”* (p. 91)
- *“How do I restart in Safe Mode?”* (p. 92)
- *“Am I using a 32 bit or a 64 bit version of Windows?”* (p. 92)
- *“How do I use System Restore in Windows?”* (p. 93)
- *“How do I display hidden objects in Windows?”* (p. 93)

### 13.1. How do I remove other security solutions?

The main reason for using a security solution is to provide protection and safety for your data. But what happens when you have more than one security product on the same system?

When you use more than one security solution on the same computer, the system becomes unstable. The Bitdefender Antivirus Plus 2012 installer automatically detects other security programs and offers you the option to uninstall them.

If you did not remove the other security solutions during the initial installation, follow these steps:

- For **Windows XP**:
  1. Click **Start**, go to **Control Panel** and double-click **Add / Remove programs**.
  2. Wait a few moments until the list of installed software is displayed.
  3. Find the name of the program you want to remove and select **Remove**.
  4. Wait for the uninstall process to complete, then reboot your system.
- For **Windows Vista** and **Windows 7**:
  1. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
  2. Wait a few moments until the installed software list is displayed.
  3. Find the name of the program you want to remove and select **Uninstall**.
  4. Wait for the uninstall process to complete, then reboot your system.

If you fail to remove the other security solution from your system, get the uninstall tool from the vendor website or contact them directly in order to provide you with the uninstall guidelines.

## 13.2. How do I restart in Safe Mode?

Safe mode is a diagnostic operating mode, used mainly to troubleshoot problems affecting normal operation of Windows. Such problems range from conflicting drivers to viruses preventing Windows from starting normally. In Safe Mode only a few applications work and Windows loads just the basic drivers and a minimum of operating system components. This is why most viruses are inactive when using Windows in Safe Mode and they can be easily removed.

To start Windows in Safe Mode:

1. Restart the computer.
2. Press the **F8** key several times before Windows starts in order to access the boot menu.
3. Select **Safe Mode** in the boot menu or **Safe Mode with Networking** if you want to have Internet access.
4. Press **Enter** and wait while Windows loads in Safe Mode.
5. This process ends with a confirmation message. Click **Ok** to acknowledge.
6. To start Windows normally, simply reboot the system.

## 13.3. Am I using a 32 bit or a 64 bit version of Windows?

To find out if you have a 32 bit or a 64 bit operating system, follow these steps:

### ● For **Windows XP**:

1. Click **Start**.
2. Locate **My Computer** on the **Start** menu.
3. Right-click **My Computer** and select **Properties**.
4. If you see **x64 Edition** listed under **System**, you are running the 64 bit version of Windows XP.

If you do not see **x64 Edition** listed, you are running a 32 bit version of Windows XP.

### ● For **Windows Vista** and **Windows 7**:

1. Click **Start**.
2. Locate **Computer** on the **Start** menu.
3. Right-click **Computer** and select **Properties**.
4. Look under **System** in order to check the information about your system.

## 13.4. How do I use System Restore in Windows?

If you cannot start the computer in normal mode, you can boot up in Safe Mode and use System Restore to restore to a time when you could start the computer without errors.

To perform the System Restore, you must be logged on to Windows as an administrator.

To use System Restore, follow these steps:

● In Windows XP:

1. Log on to Windows in Safe Mode.
2. Follow the path from the Windows start menu: **Start** → **All Programs** → **System Tools** → **System Restore**.
3. On the **Welcome to System Restore** page, click to select the **Restore my computer to an earlier time** option, and then click Next.
4. Follow the wizard steps and you should be able to boot up the system in normal mode.

● In Windows Vista and Windows 7:

1. Log on to Windows in Safe Mode.
2. Follow the path from the Windows start menu: **All Programs** → **Accessories** → **System Tools** → **System Restore**.
3. Follow the wizard steps and you should be able to boot up the system in normal mode.

## 13.5. How do I display hidden objects in Windows?

These steps are useful in those cases where you are dealing with a malware situation and you need to find and remove the infected files, which could be hidden.

Follow these steps to display hidden objects in Windows:

1. Click **Start**, go to **Control Panel** and select **Folder Options**.
2. Go to **View** tab.
3. Select **Display contents of system folders** (for Windows XP only).
4. Select **Show hidden files and folders**.
5. Clear **Hide file extensions for known file types**.
6. Clear **Hide protected operating system files**.
7. Click **Apply** and then **Ok**.

## Glossary

### **ActiveX**

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

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

### **Adware**

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

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

### **Archive**

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

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

### **Backdoor**

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

### **Boot sector**

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

### **Boot virus**

A virus that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the virus to become active in memory. Every time you boot your system from that point on, you will have the virus active in memory.

## **Browser**

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

## **Command line**

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

## **Cookie**

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

## **Disk drive**

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

A hard disk drive reads and writes hard disks.

A floppy drive accesses floppy disks.

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

## **Download**

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

## **E-mail**

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

## **Events**

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

## **False positive**

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

## **Filename extension**

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

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

## **Heuristic**

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

## **IP**

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

## **Java applet**

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

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

## **Keylogger**

A keylogger is an application that logs anything you type.

Keyloggers are not malicious in nature. They can be used for legitimate purposes, such as monitoring employees or children activity. However, they

are increasingly being used by cyber-criminals for malicious purposes (for example, to collect private data, such as login credentials and social security numbers).

## **Macro virus**

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

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

## **Mail client**

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

## **Memory**

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

## **Non-heuristic**

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

## **Packed programs**

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

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

## **Path**

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

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

## **Phishing**

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private

information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

## **Polymorphic virus**

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

## **Port**

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

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

## **Report file**

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

## **Rootkit**

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

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

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

## **Script**

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



## **Spam**

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

## **Spyware**

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

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

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

## **Startup items**

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

## **System tray**

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

## **TCP/IP**

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

## **Trojan**

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

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

## **Update**

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

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

## **Virus**

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

## **Virus signature**

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.