

Bitdefender[®] ANTIVIRUS FREE



USER'S GUIDE





Bitdefender Antivirus Free User's Guide

Publication date 02/28/2022

Copyright© 2022 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

Installation	1
1. Preparing for installation	2
2. System requirements	3
2.1. Software requirements	3
3. Installing your Bitdefender product	5
3.1. Install from Bitdefender Website	5
3.2. Install over other security solutions	9
Getting started	10
4. Bitdefender interface	11
4.1. System tray icon	11
4.2. Navigation menu	13
4.3. Dashboard	14
4.3.1. Security status area	14
4.3.2. Autopilot	15
4.3.3. Quick actions	15
4.4. The Bitdefender sections	16
4.4.1. Protection	16
4.5. Security Widget	17
4.5.1. Scanning files and folders	18
4.5.2. Hide / show Security Widget	19
4.6. Change product language	19
5. Bitdefender Central	20
5.1. Accessing Bitdefender Central	20
5.2. 2-Factor Authentication	21
5.2.1. Adding trusted devices	22
5.3. My Subscriptions	23
5.3.1. Check available subscriptions	23
5.3.2. Add a new device	23
5.3.3. Activate subscription	24
5.4. My Devices	25
5.5. Activity	26
5.6. Notifications	27
6. Keeping Bitdefender up-to-date	28
6.1. Checking if Bitdefender is up-to-date	28
6.2. Performing an update	28
6.3. Turning on or off automatic update	29
6.4. Adjusting update settings	30
6.5. Continuous updates	30
How to	32



7. Installation	33
7.1. How do I install Bitdefender on a second device?	33
7.2. How can I reinstall Bitdefender?	33
7.3. Where can I download Bitdefender Antivirus Free from?	34
7.4. How can I change the language of my Bitdefender product?	35
8. Bitdefender Central	36
8.1. How do I sign in to Bitdefender account with another account?	36
8.2. How do I turn off Bitdefender Central help messages?	36
8.3. I forgot the password I set for my Bitdefender account. How do I reset it?	37
8.4. How can I manage the logon sessions associated to my Bitdefender account?	38
9. Scanning with Bitdefender	39
9.1. How do I scan a file or a folder?	39
9.2. How do I scan my system?	39
9.3. How do I schedule a scan?	39
9.4. How do I create a custom scan task?	40
9.5. How do I except a folder from being scanned?	42
9.6. What to do when Bitdefender detected a clean file as infected?	43
9.7. How do I check what threats Bitdefender detected?	44
10. Useful Information	45
10.1. How do I test my security solution?	45
10.2. How do I remove Bitdefender?	45
10.3. How do I automatically shut down the device after the scan is over?	46
10.4. How do I configure Bitdefender to use a proxy internet connection?	47
10.5. Am I using a 32 bit or a 64 bit version of Windows?	48
10.6. How do I display hidden objects in Windows?	49
10.7. How do I remove other security solutions?	50
10.8. How do I restart in Safe Mode?	51

Managing your security **53**

11. Antivirus protection	54
11.1. On-access scanning (real-time protection)	54
11.1.1. Turning on or off real-time protection	55
11.1.2. Restoring the default settings	55
11.2. On-demand scanning	55
11.2.1. Scanning a file or folder for threats	56
11.2.2. Running a Quick Scan	56
11.2.3. Running a System Scan	56
11.2.4. Configuring a custom scan	57
11.2.5. Antivirus Scan Wizard	60
11.2.6. Checking scan logs	63
11.3. Automatic scan of removable media	64
11.3.1. How does it work?	64
11.3.2. Managing removable media scan	65
11.4. Configuring scan exceptions	65
11.4.1. Excepting files and folders from scanning	66



11.4.2. Excepting file extensions from scanning	66
11.4.3. Managing scan exceptions	67
11.5. Managing quarantined files	67
12. Advanced Threat Defense	69
12.1. Turning on or off Advanced Threat Defense	69
12.2. Checking detected malicious attacks	69
12.3. Adding processes to exceptions	70
12.4. Exploits detection	70
13. Online Threat Prevention	71
13.1. Bitdefender alerts in the browser	72
Troubleshooting	74
14. Solving common issues	75
14.1. My system appears to be slow	75
14.2. Scan doesn't start	76
14.3. I can no longer use an app	79
14.4. What to do when Bitdefender blocks a website, a domain, an IP address, or an online app that are safe	80
14.5. How to update Bitdefender on a slow internet connection	80
14.6. Bitdefender services are not responding	81
14.7. Bitdefender removal failed	82
14.8. My system doesn't boot up after installing Bitdefender	83
15. Removing threats from your system	86
15.1. What to do when Bitdefender finds threats on your device?	86
15.2. How do I clean a threat in an archive?	87
15.3. How do I clean a threat in an email archive?	89
15.4. What to do if I suspect a file as being dangerous?	89
15.5. What are the password-protected files in the scan log?	90
15.6. What are the skipped items in the scan log?	90
15.7. What are the over-compressed files in the scan log?	91
15.8. Why did Bitdefender automatically delete an infected file?	91
Contact us	92
16. Asking for help	93
17. Online resources	95
17.1. Bitdefender Support Center	95
17.2. Bitdefender Support Forum	95
17.3. HOTforSecurity Portal	96
18. Contact information	97
18.1. Web addresses	97
18.2. Local distributors	97
18.3. Bitdefender offices	97
Glossary	100



INSTALLATION



1. PREPARING FOR INSTALLATION

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

- Make sure that the device where you plan to install Bitdefender meets the system requirements. If the device does not meet all the 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, refer to "*System requirements*" (p. 3).
- Log on to the device using an Administrator account.
- Remove any other similar software from the device. If any is detected during the Bitdefender installation process, you will be notified to uninstall it. Running two security programs simultaneously may affect their operation and cause major problems with the system. Windows Defender will be disabled during the installation.



2. SYSTEM REQUIREMENTS

You may install Bitdefender Antivirus Free only on devices running the following operating systems:

- Windows 7 with Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11
- 2,5 GB available free hard disk space (at least 800 MB on the system drive)
- 2 GB of memory (RAM)
- An active internet connection



Important

System performance may be affected on devices that have old generation CPUs.



Note

To find out the Windows operating system your device is running and hardware information:

- In **Windows 7**, right-click **My Computer** on the desktop, and then select **Properties** from the menu.
- In **Windows 8**, from the Windows Start screen, locate **Computer** (for example, you can start typing "Computer" directly in the Start screen), and then right-click its icon. In **Windows 8.1**, locate **This PC**.

Select **Properties** in the bottom menu. Look in the **System** area to find information about your system type.

- In **Windows 10**, type **System** in the search box from the taskbar and click its icon. Look in the **System** area to find information about your system type.

2.1. Software requirements

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

- Microsoft Edge 40 and higher
- Internet Explorer 11 and higher



- Mozilla Firefox 51 and higher
- Google Chrome 34 and higher



3. INSTALLING YOUR BITDEFENDER PRODUCT

You can install Bitdefender using the web installer downloaded on your device from the Bitdefender Antivirus Free [page](#) on Bitdefender Website.

3.1. Install from Bitdefender Website

From Bitdefender Website you can download the Bitdefender Antivirus Free installation kit. Once the installation process is complete, Bitdefender Antivirus Free is activated.

To download Bitdefender Antivirus Free from Bitdefender Website:

1. Access <https://www.bitdefender.com/toolbox/> .
2. Click download on Bitdefender Antivirus Free.
3. Wait for the download to complete, and then run the installer.

Validating the installation

Bitdefender first checks your system to validate the installation.

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

If an incompatible security solution 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. You may need to reboot your device to complete the removal of detected security solutions.

The Bitdefender Antivirus Free installation package is constantly updated.



Note

Downloading the installation files can take a long time, especially over slower internet connections.

Once the installation is validated, the setup wizard appears. Follow the steps to install Bitdefender Antivirus Free.



Step 1 - Bitdefender installation

Before proceeding with the installation, you have to agree with the Subscription Agreement. Please take some time to read the Subscription Agreement as it contains the terms and conditions under which you may use Bitdefender Antivirus Free.

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

Two additional tasks can be performed at this step:

- Keep the **Send product reports** option enabled. By allowing this option, reports containing information about how you use the product are sent to the Bitdefender servers. This information is essential for improving the product and can help us provide a better experience in the future. Note that these reports contain no confidential data, such as your name or IP address, and that they will not be used for commercial purposes.
- Select the language you want to install the product in.

Click **INSTALL** to launch the installation process of your Bitdefender product.

Step 2 - Installation in progress

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

Step 3 - Installation completed

Your Bitdefender product is successfully installed.

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

Step 4 - Device Analysis

You will now be asked if you wish to perform an analysis of your device, to ensure that it is safe. During this step, Bitdefender will scan critical system areas. Click **Start Device Analysis** to initiate it.

You can hide the scan interface by clicking on **Run Scan in Background**. After that, choose whether you want to be informed when the scan is finished, or not.

When the scan is completed, click **Create Bitdefender Account**.



Note

Alternatively, if you do not wish to perform the scan, you can simply click on **Skip**.

Step 5 - Bitdefender account

After you complete the initial setup, the Bitdefender Account window appears. A Bitdefender account is required to activate the product and use its online features. For more information, refer to "*Bitdefender Central*" (p. 20).

Proceed according to your situation.

● I want to create a Bitdefender account

1. Type the required information in the corresponding fields. The data you provide here will remain confidential. The password must be at least 8 characters long, include at least one number or symbol and include lower and upper case characters.
2. Before proceeding further you have to agree with the Terms of use. Access the Terms of use and read them carefully as they contain the terms and conditions under which you may use Bitdefender.

Additionally, you can access and read the Privacy Policy.

3. Click **CREATE ACCOUNT**.



Note

Once the account is created, you can use the provided email address and password to sign in to your account at <https://central.bitdefender.com>, or in the Bitdefender Central app provided that it is installed on one of your Android or iOS devices. To install the Bitdefender Central app on Android, you have to access Google Play, search Bitdefender Central, and then tap the corresponding installation option. To install the Bitdefender Central app on iOS, you have to access App Store, search Bitdefender Central, and then tap the corresponding installation option.

● I already have a Bitdefender account

1. Click **Sign In**.
2. Type the email address in the corresponding field, and then click **NEXT**.
3. Type your password, and then click **SIGN IN**.



If you forgot the password for your account or you simply want to reset the one you already set:

- a. Click **Forgot password?**
- b. Type your email address, and then click **NEXT**.
- c. Check your email account, type the security code you have received, and then click **NEXT**.

Alternatively, you can click **Change password** in the email that we sent you.

- d. Type the new password you want to set, and then type it once again. Click **SAVE**.



Note

If you already have a MyBitdefender account, you can use it to sign into your Bitdefender account. If you forgot your password, you first need to go to <https://my.bitdefender.com> to reset it. Then, use the updated credentials to sign into your Bitdefender account.

● I want to sign in using my Microsoft, Facebook or Google account

To sign in with your Microsoft, Facebook or Google account:

1. Select the service you want to use. 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 sign in, or the personal information of your friends and contacts.

Step 6 - Activate your product



Note

This step appears if you have selected to create a new Bitdefender account during the previous step, or if you signed in using an account with an expired subscription.



An active internet connection is required to complete the activation of your product.

If you already have an active subscription on your account, that subscription will be used to protect your device.

If you do not have an active subscription, your Bitdefender Antivirus Free will be activated. You can also opt-in for a 30 days Bitdefender Total Security trial.

Step 7 - Get started

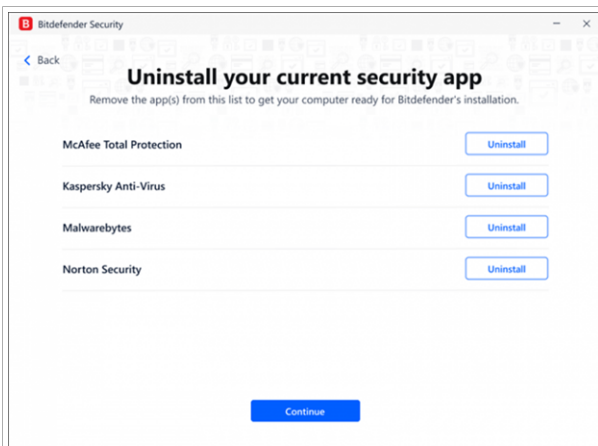
In the **Get started** window you can see details about your active subscription.

Click **FINISH** to access the Bitdefender Antivirus Free interface.

3.2. Install over other security solutions

Having multiple security solutions on your device can cause system malfunction such as slowdowns or crashes.

To ensure your device will not be affected by having multiple security solutions on it, in the installation process Bitdefender Antivirus Free will guide you through the uninstall of the existing security solutions detected.



Installing Bitdefender



GETTING STARTED



4. BITDEFENDER INTERFACE

Bitdefender Antivirus Free 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 go through the Bitdefender interface, an introduction wizard containing details on how to interact with the product and how to configure it is displayed on the upper left side. Select the right angle bracket to continue being guided, or **Skip tour** to close the wizard.

The Bitdefender **system tray icon** is available at any time, no matter whether you want to open the main window, run a product update, or view information about the installed version.

The main window gives you information about your security status. Based on your device usage and needs, **Autopilot** displays here different types of recommendations to help you improve your device security and performance. Moreover, you can add quick actions that you use the most, so that you can have them at hand whenever you need.

From the navigation menu on the left side you can access the settings area, notifications and the **Bitdefender sections** for detailed configuration and advanced administrative tasks.

From the upper part of the main interface, you can access your **Bitdefender account**. Also, you can contact us for support in case you have questions or something unexpected appears.

If you want to keep a constant eye on essential security information and have quick access to key settings, add the **Security Widget** to your desktop.

4.1. System tray icon

To manage the entire product more quickly, you can use the Bitdefender **B** icon in the system tray.



Note

The Bitdefender icon may not be visible at all times. To make the icon appear permanently:

- In **Windows 7, Windows 8 and Windows 8.1**:

1. Click the arrow  in the lower-right corner of the screen.



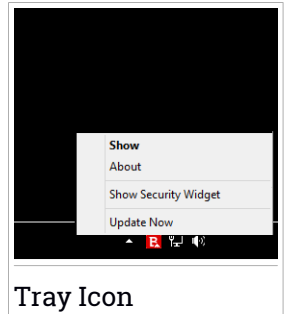
2. Click **Customize...** to open the Notification Area Icons window.
3. Select the option **Show icons and notifications** for the **Bitdefender agent** icon.

● **In Windows 10:**

1. Right-click the taskbar and select **Taskbar settings**.
2. Scroll down and click the **Select which icons appear on the taskbar** link under **Notification area**.
3. Enable the switch next to **Bitdefender agent**.

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, where to look for help in case something unexpected appears, where to access and view the Subscription Agreement, 3rd Party Components and Privacy Policy.
- **Hide / Show Security Widget** - enables / disables **Security Widget**.
- **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 device or how the product operates, by displaying a special symbol, as follows:


- R**. No issues are affecting the security of your system.
- R**. Critical issues are affecting the security of your system. They require your immediate attention and must be fixed as soon as possible.

If Bitdefender is not working, the system tray icon appears on a gray background: **B**. This usually happens when the subscription expires. It can also occur when the Bitdefender services are not responding or when other errors affect the normal operation of Bitdefender.




4.2. Navigation menu

On the left side of the Bitdefender interface is the navigation menu, which enables you to quickly access the Bitdefender features and tools you need to handle your product. The tabs available in this area, are:

-  **Dashboard.** From here, you can quickly fix security issues, view recommendations according to your system needs and usage patterns, and perform quick actions.




-  **Protection.** From here, you can launch and configure antivirus scans, recover data in case it gets encrypted by a ransomware, and configure protection while surfing on the internet.



Note


Some features are not available on the free version.

-  **Privacy.** From here, you can create password managers for your online accounts, make online payments in a safe environment, and open the VPN app.



Note


Some features are not available on the free version.


-  **Utilities.** From here, you can manage profiles and access the Data Protection feature.



Note



Some features are not available on the free version.

-  **Notifications.** From here, you have access to the generated notifications.

-  **Settings.** From here, you have access to general settings.

On the upper side of the main interface, you will find the **My Account** and **Support** features.



-  **Support.** From here, whenever you need assistance in solving a situation with your Bitdefender Antivirus Free, you can contact the Bitdefender Technical Support department.
-  **My Account.** From here, you can access your Bitdefender account to verify your subscriptions and perform security tasks on the devices you manage. Details about the Bitdefender account and in use subscription are available as well.

4.3. Dashboard

The Dashboard window allows you to perform common tasks, quickly fix security issues, view information about product operation and access the panels from where you configure the product settings.

Everything is just a few clicks away.

The window is organized in three main areas:

Security status area

This is where you can check your device's security status.

Autopilot

This is where you can check the Autopilot recommendations to ensure proper functionality of the system.

Quick actions

This is where you can run different tasks to keep your system protected.




Note

Some tasks are not available on the free version.

4.3.1. Security status area

Bitdefender uses an issue tracking system to detect and inform you about the issues that may affect the security of your device and data. Detected issues include important protection settings that are turned off and other conditions that can represent a security risk.

Whenever issues are affecting the security of your device, the status that appears on the upper side of the **Bitdefender interface** changes into red. The displayed status indicates the nature of issues affecting your system. Also, the **system tray** icon changes into  and if you move the mouse cursor over the icon, a pop-up will confirm the existence of pending issues.



As the detected issues may prevent Bitdefender from protecting you against threats or represent a major security risk, we recommend you to pay attention and fix them as soon as possible. To fix an issue, click the button next to the detected issue.

4.3.2. Autopilot

To offer you an effective operation and increased protection while carrying out different activities, Bitdefender Autopilot will act as your personal security advisor. Depending on the activity you perform, either you work, make online payments, watch movies, or play games Bitdefender Autopilot will come up with contextual recommendations based on your device usage and needs. The proposed recommendations may also be related to actions that you need to perform to keep your product working at its full capacity.

To start using a suggested feature or make improvements into your product, click the corresponding button.

Turning off Autopilot notifications

To bring your attention to the Autopilot recommendations, the Bitdefender product is set up to notify you through a pop-up window.


To turn off the Autopilot notifications:

1. Click **Settings** on the navigation menu on the **Bitdefender interface**.
2. In the **General** window, turn off **Recommendation notifications**.

4.3.3. Quick actions

Using quick actions you can quickly launch tasks that you consider important for keeping your system protected and improving the way you work.

By default, Bitdefender comes with some quick actions that can be replaced with the ones you know you mostly use. To replace a quick action:

1. Click the  icon in the upper-right corner of the card you want to remove.
2. Point the task you want to add to the main interface, and then click **ADD**.

The tasks you can add to the main interface, are:

- **Quick Scan.** Run a quick scan to promptly detect the possible threats that may be present on your device.



- **System Scan.** Run a system scan to make sure your device is clean of threats.

To start protecting additional Windows devices:

1. Click **Install Bitdefender on another device.**

A new window appears on your screen.

2. Click **SHARE DOWNLOAD LINK.**
3. Follow the on-screen steps to install Bitdefender Antivirus Free on Windows-based devices.

4.4. The Bitdefender sections

4.4. The Bitdefender sections

The Bitdefender product comes with three sections divided into useful features to help you stay protected while you work, surf the web or perform online payments, improve the speed of your system and many more.

Whenever you want to access the features for a specific section or to start configuring your product, access the following icons located on the navigation menu on the **Bitdefender interface**:

-  **Protection**
-  **Privacy**
-  **Utilities**

4.4.1. Protection

In the Protection section you can configure security settings or configure and run scan tasks.

The features you can manage in the Protection section are:

ANTIVIRUS

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

From the Antivirus feature you can easily access the following scan tasks:

- Quick Scan



- System Scan
- Manage Scans

For more information about scan tasks and how to configure antivirus protection, refer to *"Antivirus protection"* (p. 54).

ONLINE THREAT PREVENTION

Online Threat Prevention helps you to stay protected against phishing attacks, fraud attempts and private data leaks, while surfing on the internet.

For more information about how to configure Bitdefender to protect your web activity, refer to *"Online Threat Prevention"* (p. 71).

ADVANCED THREAT DEFENSE

Advanced Threat Defense actively protects your system against threats such as ransomware, spyware and trojans by analyzing the behavior of all installed apps. Suspicious processes are identified and, when necessary, blocked.

For more information about how to keep your system protected from threats, refer to *"Advanced Threat Defense"* (p. 69).

4.5. Security Widget

Security Widget is the quick and easy way to monitor and control Bitdefender Antivirus Free. Adding this small and unintrusive widget to your desktop lets you see critical information and perform key tasks at all times:

- open the main window of Bitdefender.
- monitor scanning activity in real-time.
- monitor the security status of your system and fix any existing issues.
- view when an update is in progress.
- view notifications and get access to the latest events reported by Bitdefender.
- scan files or folders by dragging and dropping one or multiple items over the widget.



The overall security status of your computer is displayed **at the center** of the widget. The status is indicated by the color and shape of the icon that is displayed in this area.



Your system is currently at risk.

They require your immediate attention and must be fixed as soon as possible. Click the status icon to begin fixing the reported issues.



Bitdefender services are not responding.



Your system is protected.



When a scan task is in progress, this animated icon is displayed.



This icon indicates that your Bitdefender subscription has expired.



When an update is in progress, this icon is displayed.

When issues are reported, click the status icon to launch the Fix Issues wizard.

The lower side of the widget displays the unread events counter (the number of outstanding events reported by Bitdefender, if any). Click the event counter, for example **1** for one unread event, to open the Notifications window. For more information, refer to [???](#).

4.5.1. Scanning files and folders

You can use the Security Widget to quickly scan files and folders. Drag any file or folder you want to be scanned and drop it over the **Security Widget**.



The **Antivirus Scan wizard** will appear and guide you through the scanning process. The scanning options are pre-configured for the best detection results and can not be changed. If infected files are detected, Bitdefender will try to disinfect them (remove the malicious code). If disinfection fails, the Antivirus Scan wizard will allow you to specify other actions to be taken on infected files.

4.5.2. Hide / show Security Widget

When you no longer want to see the widget, click **✕**.

To restore Security Widget, use one of the following methods:

● From system tray:

1. Right-click the Bitdefender icon in the **system tray**.
2. Click **Show Security Widget** in the contextual menu that appears.

● From the Bitdefender interface:

1. Click **Settings** on the navigation menu on the **Bitdefender interface**.
2. In the **General** window, turn on **Security Widget**.

The Bitdefender Security Widget is disabled by default.

4.6. Change product language

The Bitdefender interface is available in several languages and can be changed by following these steps:

1. Click **Settings** on the navigation menu on the **Bitdefender interface**.
2. In the **General** window, click **Change Language**.
3. Select the desired language from the list, and then click **SAVE**.
4. Wait a few moments until the settings are applied.



5. BITDEFENDER CENTRAL

Bitdefender Central is the platform where you have access to the product's online features and services and can remotely perform important tasks on devices Bitdefender is installed on. You can sign in to your Bitdefender account from any device connected to the internet by going to <https://central.bitdefender.com>, or directly from the Bitdefender Central app on Android and iOS devices.

To install the Bitdefender Central app on your devices:


- **On Android** - search Bitdefender Central on Google Play, and then download and install the app. Follow the required steps to complete the installation.
- **On iOS** - search Bitdefender Central on App Store, and then download and install the app. Follow the required steps to complete the installation.

Once you are signed in, you can start doing the following:

- Download and install Bitdefender on Windows based devices.
- Add new devices to your network and manage them wherever you are.

5.1. Accessing Bitdefender Central

There are several ways to access Bitdefender Central:

- From the Bitdefender main interface:
 1. Click the  icon in the upper right side of the **Bitdefender interface**.
 2. Click **Go to Bitdefender Central**.
 3. Sign in to your Bitdefender account using your email address and password.
- From your web browser:
 1. Open a web browser on any device with internet access.
 2. Go to: <https://central.bitdefender.com>.
 3. Sign in to your Bitdefender account using your email address and password.
- From your Android or iOS-based device:

Open the Bitdefender Central app you have installed.



Note

In this material you are provided with the options and instructions available on the web platform.


5.2. 2-Factor Authentication

The 2-Factor Authentication method adds an extra security layer to your Bitdefender account, by requiring an authentication code in addition to your sign-in credentials. This way you will prevent account takeover and keep away types of cyberattacks, such as keyloggers, brute-force or dictionary attacks.

Enabling 2-Factor Authentication

By enabling 2-Factor Authentication, you will make your Bitdefender account much more secure. Your identity will be verified each time you will sign in from different devices, either to install one of the Bitdefender products, check the status of your subscription or run tasks remotely on your devices.

To enable 2-Factor Authentication:

1. Access **Bitdefender Central**.
2. Click the  icon in the upper right side of the screen.
3. Click **Bitdefender Account** in the slide menu.
4. Select the **Password and security** tab.
5. Click **2-Factor Authentication**.
6. Click **GET STARTED**.

Choose one of the following methods:

- **Authenticator App** - use an authenticator app to generate a code each time you want sign in to your Bitdefender account.

If you would like to use an authenticator app, but you are not sure what to choose, a list with the authentication apps we recommend is available.

- a. Click **USE AUTHENTICATOR APP** to start.
- b. To sign in on an Android or iOS-based device, use your device to scan the QR code.



To sign in on a laptop or a desktop, you can add manually the displayed code.

Click **CONTINUE**.

c. Insert the code provided by the app or the one displayed at the previous step, and then click **ACTIVATE**.

● **E-mail** - each time you sign in to your Bitdefender account, a verification code will be sent to your email inbox. Check your email account, and then type in the code you have received.

a. Click **USE EMAIL** to start.

b. Check your email account and type in the provided code.

Note that you have five minutes to check your email account and type in the generated code. If the time expires, you will have to generate a new code by following the same steps.

c. Click **ACTIVATE**.

d. You are provided with ten activation codes. You can either copy, download, or print the list and use it in case you lose your email address or will not be able to sign in. Each code can only be used once.

e. Click **DONE**.

In case you want to stop using 2-Factor Authentication:

1. Click **TURN OFF 2-FACTOR AUTHENTICATION**.

2. Check your app or email account and type in the code you have received.

In case you have chosen to receive the authentication code via email, you have five minutes to check your email account and type in the generated code. If the time expires, you will have to generate a new code by following the same steps.


3. Confirm your choice.

5.2.1. Adding trusted devices

To make sure that only you can access your Bitdefender account, we might require a security code first. If you would like to skip this step each time you connect from the same device, we recommend you to nominate it as a trusted device.



To add devices as trusted devices:

1. Access **Bitdefender Central**.
2. Click the  icon in the upper right side of the screen.
3. Click **Bitdefender Account** in the slide menu.
4. Select the **Password and security** tab.
5. Click **Trusted Devices**.
6. The list with the devices Bitdefender is installed on is displayed. Click the desired device.

You can add as many devices as you want, provided that they have Bitdefender installed and your subscription is valid.

5.3. My Subscriptions

The Bitdefender Central platform gives you the possibility to easily see the subscriptions you have for all your devices.

5.3.1. Check available subscriptions

To check your available subscriptions:

1. Access **Bitdefender Central**.
2. Select the **My Subscriptions** panel.

Here you have information about the availability of the subscriptions you own and the number of devices using each of them.




Note

You can have one or more subscriptions on your account provided that they are for different platforms (Windows, macOS, iOS or Android).

5.3.2. Add a new device

If your subscription covers more than one device, you can add a new device and install your Bitdefender Antivirus Free on it, as follows:

1. Access **Bitdefender Central**.
2. Select the **My Devices** panel, and then click the  icon.
3. Choose one of the two available options:



● **Protect this device**

Select this option, and then select the owner of the device. If the device belongs to someone else, click the corresponding button.

● **Protect other devices**

Select this option, and then select the owner of the device. If the device belongs to someone else, click the corresponding button.

Click **SEND DOWNLOAD LINK**. Type an email address in the corresponding field, and click **SEND EMAIL**. Note that the generated download link is valid for the next 24 hours only. If the link expires, you will have to generate a new one by following the same steps.

On the device you want to install your Bitdefender product, check the email account that you typed in, and then click the corresponding download button.

4. Wait for the download to complete, and then run the installer.


5.3.3. Activate subscription

A paid subscription can be activated during the installation process by using your Bitdefender account. Together with the activation process, its validity starts to count-down.

If you have purchased an activation code from one of our resellers or you received it as a present, then you can add its availability to any existing Bitdefender subscription available on the account, provided that they are for the same product.

To activate a subscription using an activation code:

1. Access **Bitdefender Central**.
2. Select the **My Subscriptions** panel.
3. Click the **+Activate with code** button, then type the code in the corresponding field.
4. Click **ACTIVATE** to continue.

The subscription is now activated. Go to **My Devices** panel, and click the  icon to install the product on one of your devices.



Note


If you activate a subscription with activation code, the existing free subscription will be replaced with the paid subscription.

5.4. My Devices


The **My Devices** area in Bitdefender Central gives you the possibility to install, manage and take remote actions on your Bitdefender product on any device, provided that it is turned on and connected to the internet. The device cards display the device name, the operating system, the products installed, the protection status and if there are security risks affecting the protection of your devices.

To view a list of your devices sorted according to their status or users, click the drop-down arrow in the upper-right corner of the screen.

To easily identify your devices, you can customize the device name:


1. Access **Bitdefender Central**.
2. Select the **My Devices** panel.
3. Click **VIEW DETAILS** on the desired device card, and then the  icon in the upper-right corner of the screen.
4. Select **Settings**.
5. Type in a new name in the **Device name** field, then click **SAVE**.

You can create and assign an owner to each of your devices for better management:

1. Access **Bitdefender Central**.
2. Select the **My Devices** panel.
3. Click **VIEW DETAILS** on the desired device card, and then the  icon in the upper-right corner of the screen.
4. Select **Profile**.
5. Click **Add owner**, then fill in the corresponding fields. Customize the profile by adding a photo and selecting a date of birth.
6. Click **ADD** to save the profile.
7. Select the desired owner from the **Device owner** list, then click **ASSIGN**.



To remotely update Bitdefender on a Windows device:

1. Access **Bitdefender Central**.
2. Select the **My Devices** panel.
3. Click **VIEW DETAILS** on the desired device card, and then the  icon in the upper-right corner of the screen.
4. Select **Update**.

For more remote actions and information regarding your Bitdefender product on a specific device, click **VIEW DETAILS** on the desired device card.

Once you click **VIEW DETAILS** on a device card, the following tabs are available:

- **Dashboard.** In this window you can view details about the selected device, check its protection status and how many threats have been blocked in the last seven days. The protection status can be green, when there is no issue affecting your device, yellow when the device needs your attention or red when the device is at risk. When there are issues affecting your device, click the drop-down arrow in the upper status area to find out more details. From here you can manually fix issues that are affecting the security of your devices.
- **Protection.** From this window you can remotely run a Quick or a System Scan on your devices. Click the **SCAN** button to start the process. You can also check when the last scan was performed on the device and a report of the latest scan with the most important information is available. For more information about these two scan processes, refer to [Section 11.2.3, "Running a System Scan"](#) and to ["Running a Quick Scan" \(p. 56\)](#).

5.5. Activity

In the Activity area you have access to information on the devices that have Bitdefender installed.

Once you access the **Activity** window, the following cards are available:

- **My Devices.** Here you can view the number of the connected devices along with their protection status. To fix issues remotely on the detected devices, click **Fix issues**, and then click **SCAN AND FIX ISSUES**.

To view details about the detected issues, click **View issues**.



Information about detected threats cannot be retrieved from iOS-based devices.

- **Threats blocked.** Here you can view a graph showing an overall statistic including information about the threats blocked in the last 24 hours and seven days. The displayed information is retrieved depending on the malicious behavior detected on accessed files, apps and URLs.
- **Top users with threats blocked.** Here you can view a top with the users were the most threats have been found.
- **Top devices with threats blocked.** Here you can view a top with the devices were the most threats have been found.

5.6. Notifications

To help you stay informed about what is happening on the devices associated to your account, the 🔔 icon is at hand. Once you click it you have an overall image consisting of information about the activity of the Bitdefender products installed on your devices.



6. KEEPING BITDEFENDER UP-TO-DATE

New threats are found and identified every day. This is why it is very important to keep Bitdefender up to date with the latest threat information database.

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 device and every **hour** after that. If an update is detected, it is automatically downloaded and installed on your device.

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



Important

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

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

- If your device 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. 47).
- 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, refer to *"Performing an update"* (p. 28).

6.1. Checking if Bitdefender is up-to-date

To check the time of the last update of your Bitdefender:


1. Click **Notifications** on the navigation menu on the **Bitdefender interface**.
2. In the **All** tab, select the notification regarding the latest update.

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.

6.2. Performing an update

To perform updates, an internet connection is required.



To start an update, right-click the Bitdefender  icon in the **system tray**, and then select **Update Now**.

The Update feature 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 device when you have completed the update. We recommend doing it as soon as possible.

You can also perform updates remotely on your devices, provided that they are turned on and connected to the internet.

To remotely update Bitdefender on a Windows device:

1. Access **Bitdefender Central**.
2. Select the **My Devices** panel.
3. Click **VIEW DETAILS** on the desired device card, and then the  icon in the upper-right corner of the screen.
4. Select **Update**.

6.3. Turning on or off automatic update

To turn on or off automatic update:

1. Click **Settings** on the navigation menu on the **Bitdefender interface**.
2. Select the **Update** tab.
3. Turn on or off the corresponding switch.
4. A warning window appears. 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 or until a 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.



6.4. 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:

1. Click **Settings** on the navigation menu on the **Bitdefender interface**.
2. Select the **Update** tab and adjust the settings according to your preferences.

Update frequency

Bitdefender is configured to check for updates every hour. To change the update frequency, drag the slider along the scale to set the desired period of time when the update should occur.

Update processing rules

Every time an update is available, Bitdefender will automatically download and implement the update without showing notifications. Turn off the **Silent update** option if you want to be notified each time a new update is available.

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 device. 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 on **Restart notification**.

6.5. Continuous updates

To make sure that you are using the latest version, your Bitdefender automatically checks for product updates. These updates may bring new features and improvements, fix product issues, or automatically upgrade you to a new version. When the new Bitdefender version comes via update,



customized settings are saved, and the uninstall and reinstall procedure is skipped.

These updates require a system restart to initiate the installation of new files. When a product update is completed, a pop-up window will inform you to restart the system. If you miss this notification, you can either click **RESTART NOW** in the **Notifications** window where the most recent update is mentioned, or manually restart the system.



HOW TO



7. INSTALLATION

7.1. How do I install Bitdefender on a second device?

If the subscription covers more than one device, you can use your Bitdefender account to activate a second PC.

To install Bitdefender on a second device:

1. Click **Install Bitdefender on another device** on the lower-left corner of the **Bitdefender interface**.

A new window appears on your screen.

2. Click **SHARE DOWNLOAD LINK**.
3. Follow the on-screen instructions to install Bitdefender.

The new device on which you have installed the Bitdefender product will appear in the Bitdefender Central dashboard.

7.2. How can I reinstall Bitdefender?

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

- you have reinstalled the operating system.
- you want to fix issues that might have caused slowdowns and crashes.
- your Bitdefender product is not starting or working properly.

In case one of the mentioned situations is your case, follow these steps:

- In **Windows 7**:

1. Click **Start** and go to **All Programs**.
2. Find **Bitdefender Antivirus Free** and select **Uninstall**.
3. Click **REINSTALL** in the window that appears.
4. You need to restart the device to complete the process.

- In **Windows 8 and Windows 8.1**:

1. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen), and then click its icon.



2. Click **Uninstall a program** or **Programs and Features**.
3. Find **Bitdefender Antivirus Free** and select **Uninstall**.
4. Click **REINSTALL** in the window that appears.
5. You need to restart the device to complete the process.

● In **Windows 10**:

1. Click **Start**, then click Settings.
2. Click the **System** icon in the Settings area, then select **Apps & features**.
3. Find **Bitdefender Antivirus Free** and select **Uninstall**.
4. Click **Uninstall** again to confirm your choice.
5. Click **REINSTALL**.
6. You need to restart the device to complete the process.



Note

By following this reinstall procedure, customized settings are saved and available in the new installed product. Other settings may be switched back to their default configuration.

7.3. Where can I download Bitdefender Antivirus Free from?

You can download Bitdefender Antivirus Free from the Bitdefender Website. Once the installation process is complete, Bitdefender Antivirus Free is activated.



Note

Before running the kit, it is recommended to remove any security solution installed on your system. When you use more than one security solution on the same device, the system becomes unstable.

To download Bitdefender Antivirus Free from Bitdefender Website::

1. Access <https://www.bitdefender.com/toolbox/>.
2. Click download on Bitdefender Antivirus Free.
3. Wait for the download to complete, and then run the installer.
4. Run the Bitdefender product you have downloaded.



7.4. How can I change the language of my Bitdefender product?

The Bitdefender interface is available in several languages and can be changed by following these steps:

1. Click **Settings** on the navigation menu on the **Bitdefender interface**.
2. In the **General** window, click **Change Language**.
3. Select the desired language from the list, and then click **SAVE**.
4. Wait a few moments until the settings are applied.



8. BITDEFENDER CENTRAL

8.1. How do I sign in to Bitdefender account with another account?

You have created a new Bitdefender account and you want to use it from now on.

To successfully sign in with another Bitdefender account:

1. Click on your account name in the upper part of the **Bitdefender interface**.
2. Click **Switch Account** on the upper right corner of the screen to change the account linked to the device.
3. Type the email address in the corresponding field, and then click **NEXT**.
4. Type your password, and then click **SIGN IN**.




Note

The Bitdefender product from your device automatically changes according to the subscription associated to the new Bitdefender account. If there is no available subscription associated to the new Bitdefender account, or you wish to transfer it from the previous account, you can contact Bitdefender for support as described in section *"Asking for help"* (p. 93).

8.2. How do I turn off Bitdefender Central help messages?

To help you understand what each option in Bitdefender Central is useful for, help messages are displayed in the dashboard.

If you wish to stop seeing this kind of messages:


1. Access **Bitdefender Central**.
2. Click the  icon in the upper right side of the screen.
3. Click **My Account** in the slide menu.
4. Click **Settings** in the slide menu.
5. Disable the **Turn on/off help messages** option.



8.3. I forgot the password I set for my Bitdefender account. How do I reset it?

There are two possibilities to set a new password for your Bitdefender account:

- From the **Bitdefender interface**:

1. Click the  icon in the upper right side of the **Bitdefender interface**.
2. Click **Switch Account** on the upper right corner of the screen.
A new window appears.
3. Type your email address and click **NEXT**.
A new window appears.
4. Click **Forgot password?**.
5. Click **NEXT**.
6. Check your email account, type the security code you have received, and then click **NEXT**.
Alternatively, you can click **Change password** in the email that we sent you.
7. Type the new password you want to set, and then type it once again.
Click **SAVE**.

- From your web browser:

1. Go to: <https://central.bitdefender.com>.
2. Click **SIGN IN**.
3. Type your email address, and then click **NEXT**.
4. Click **Forgot password?**.
5. Click **NEXT**.
6. Check your email account and follow the provided instructions to set a new password for your Bitdefender account.

To access your Bitdefender account from now on, type your email address and the new password you have just set.



8.4. How can I manage the logon sessions associated to my Bitdefender account?

In your Bitdefender account you have the possibility to view the latest inactive and active logon sessions running on devices associated to your account. Moreover, you can sign out remotely by following these steps:

1. Access **Bitdefender Central**.
2. Click the 👤 icon in the upper right side of the screen.
3. Click **Sessions** in the slide menu.
4. In the **Active sessions** area, select the **SIGN OUT** option next to the device you want to finish the logon session.



9. SCANNING WITH BITDEFENDER

9.1. How do I scan a file or a folder?

The easiest way to scan a file or folder is to right-click the object you want to scan, point to Bitdefender and select **Scan with Bitdefender** from the menu.

To complete the scan, follow the Antivirus Scan wizard. Bitdefender will automatically take the recommended actions on detected files.

If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

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 files from the internet that you think might be dangerous.
- Scan a network share before copying files to your device.

9.2. How do I scan my system?

To perform a complete scan on the system:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ANTIVIRUS** pane, click **Open**.
3. Click the **Run Scan** button next to **System Scan**.
4. Follow the System Scan wizard to complete the scan. Bitdefender will automatically take the recommended actions on detected files.


If there remain unresolved threats, you will be prompted to choose the actions to be taken on them. For more information, refer to "*Antivirus Scan Wizard*" (p. 60).

9.3. How do I schedule a scan?

You can set your Bitdefender product to start scanning important system locations when you are not in the front of the device.

To schedule a scan:



1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ANTIVIRUS** pane, click **Open**.
3. Click  next to the scan type that you want to schedule, System Scan or Quick Scan, in the lower part of the interface, then select **Edit**.
Alternatively, you can create a scan type to suit your needs by clicking **+Create Scan** next to **Manage Scans**.
4. Customize the scan according to your needs, then click **Next**.
5. Check the box next to **Choose when to schedule this task**.

Select one of the corresponding options to set a schedule:

- At system startup
- Daily
- Weekly
- Monthly

If you choose Daily, Monthly, or Weekly, drag the slider along the scale to set the desired period of time when the scheduled scan should start.

If you choose to create a new custom scan, the **Scan task** window appears. From here you can select the locations you want to be scanned.

9.4. How do I create a custom scan task?

If you want to scan specific locations on your device or to configure the scanning options, configure and run a customized scan task.

To create a customized scan task, proceed as follows:

1. In the **ANTIVIRUS** pane, click **Open**.
2. Click **+Create Scan** next to **Manage Scans**.
3. In the task name field, type a name for the scan, select the locations you would like to be scanned, and then click **NEXT**.
4. Configure these general options:
 - Scan only applications**. You can set Bitdefender to scan only accessed apps.



- **Scan task priority.** You can choose the impact a scan process should have on your system performance.
 - Auto - The priority of the scan process will depend on the system activity. To make sure that the scan process will not affect the system activity, Bitdefender will decide whether the scan process should be run with high or low priority.
 - High - The priority of the scan process will be high. By choosing this option, you will allow other programs to run slower and decrease the time needed for the scan process to finish.
 - Low - The priority of the scan process will be low. By choosing this option, you will allow other programs to run faster and increase the time needed for the scan process to finish.
 - **Post scan actions.** Choose what action Bitdefender should take in case no threats are found:
 - Show Summary window
 - Shutdown device
 - Close Scan window
5. If you want to configure the scanning options in detail, click **Show advanced options**.
Click **Next**.
6. You can enable the **Schedule scan task** option, if you wish, then choose when the custom scan you created should start.
- At system startup
 - Daily
 - Monthly
 - Weekly
- If you choose Daily, Monthly, or Weekly, drag the slider along the scale to set the desired period of time when the scheduled scan should start.
7. Click **Save** to save the settings and close the configuration window.
- Depending on the locations to be scanned, the scan may take a while. If threats will be found during the scanning process, you will be prompted to choose the actions to be taken on the detected files.



If you want to, you can quickly rerun a previous custom scan by clicking the corresponding entry in the available list.

9.5. How do I except a folder from being scanned?

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

Exceptions 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 apps for testing purposes. Scanning the folder may result in losing some of the data.

To add a folder to the Exceptions list:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ANTIVIRUS** pane, click **Open**.
3. Click the **Settings** tab.
4. Click on **Manage Exceptions**.
5. Click **+Add an Exception**.
6. Enter the path of the folder you want to except from scanning in the corresponding field.

Alternatively, you can navigate to the folder by clicking the browse button in the right side of the interface, select it and click on **OK**.

7. Turn on the switch next to the protection feature that should not scan the folder. There are three options:
 - Antivirus
 - Online Threat Prevention
 - Advanced Threat Defense
8. Click **Save** to save the changes and close the window.



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

There may be 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 Exceptions area:

1. Turn off the Bitdefender real-time antivirus protection:
 - a. Click **Protection** on the navigation menu on the **Bitdefender interface**.
 - b. In the **ANTIVIRUS** pane, click **Open**.
 - c. In the **Advanced** window, turn off **Bitdefender Shield**.

A warning window appears. 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 a system restart.
2. Display hidden objects in Windows. To find out how to do this, refer to *"How do I display hidden objects in Windows?"* (p. 49).
3. Restore the file from the Quarantine area:
 - a. Click **Protection** on the navigation menu on the **Bitdefender interface**.
 - b. In the **ANTIVIRUS** pane, click **Open**.
 - c. Go to the **Settings** windows and click **Manage quarantine**.
 - d. Select the file, and then click **Restore**.
4. Add the file to the Exceptions list. To find out how to do this, refer to *"How do I except a folder from being scanned?"* (p. 42).

By default, Bitdefender is to automatically add restored files to the exceptions list.
5. Turn on the Bitdefender real-time antivirus protection.
6. Contact our support representatives so that we may remove the detection of the threat information update. To find out how to do this, refer to *"Asking for help"* (p. 93).



9.7. How do I check what threats Bitdefender detected?

Each time a scan is performed, a scan log is created and Bitdefender records the detected issues.

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 a scan log or any detected infection at a later time:

1. Click **Notifications** on the navigation menu on the **Bitdefender interface**.
2. In the **All** tab, select the notification regarding the latest scan.

This is where you can find all threat scan events, including threats detected by on-access scanning, user-initiated scans and status changes for automatic scans.

3. In the notifications list, you can check what scans have been performed recently. Click a notification to view details about it.
4. To open a scan log, click **View log**.



10. USEFUL INFORMATION

10.1. How do I test my security solution?

To make sure that your Bitdefender product is properly running, we recommend you using the Eicar test.

The Eicar test allows you to check your security solution using a safe file developed for this purpose.

To test your security solution:

1. Download the test from the official webpage of the EICAR organization <http://www.eicar.org/>.
2. Click the **Anti-Malware Testfile** tab.
3. Click **Download** on the left-side menu.
4. From **Download area using the standard protocol http** click the **ecar.com** test file.
5. You will be informed that the page you are trying to access contains the EICAR-Test-File (not a threat).

If you click **I understand the risks, take me there anyway**, the download of the test will begin and a Bitdefender pop-up will inform you that a threat was detected.

Click **More details** to find out more information about this action.

If you do not receive any Bitdefender alert, we recommend you to contact Bitdefender for support as described in section "*Asking for help*" (p. 93).

10.2. How do I remove Bitdefender?

If you want to remove your Bitdefender Antivirus Free:

● In **Windows 7**:

1. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
2. Find **Bitdefender Antivirus Free** and select **Uninstall**.
3. Click **REMOVE** in the window that appears.
4. Wait for the uninstall process to complete, and then reboot your system.

● In **Windows 8 and Windows 8.1**:



1. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen), and then click its icon.
2. Click **Uninstall a program** or **Programs and Features**.
3. Find **Bitdefender Antivirus Free** and select **Uninstall**.
4. Click **REMOVE** in the window that appears.
5. Wait for the uninstall process to complete, and then reboot your system.

● In **Windows 10**:

1. Click **Start**, then click Settings.
2. Click the **System** icon in the Settings area, then select **Apps**.
3. Find **Bitdefender Antivirus Free** and select **Uninstall**.
4. Click **Uninstall** again to confirm your choice.
5. Click **REMOVE** in the window that appears.
6. Wait for the uninstall process to complete, and then reboot your system.



Note

This reinstall procedure will permanently delete the customized settings.

10.3. How do I automatically shut down the device after the scan is over?

Bitdefender offers multiple scan tasks that you can use to make sure your system is not infected with threats. Scanning the entire device may take longer time to complete depending on your system's hardware and software configuration.


For this reason, Bitdefender allows you to configure your product to shut down your system as soon as the scan is over.

Consider this example: you have finished your work and you want to go to sleep. You would like to have your entire system checked for threats by Bitdefender.

To shut down the device when Quick Scan or System scan is over:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ANTIVIRUS** pane, click **Open**.




3. In the **Scans** window, click  next to Quick Scan or System Scan and select **Edit**.
4. Customize the scan according to your needs and click **Next**.
5. Check the box next to **Choose when to schedule this task**, and then choose when the task should start.

If you choose Daily, Monthly, or Weekly, drag the slider along the scale to set the desired period of time when the scheduled scan should start.

6. Click **Save**.

To shut down the device when a custom scan is over:

1. Click  next to the custom scan you created.
2. Click **Next** and then click **Next** again.
3. Check the box next to **Choose when to schedule this task**, and then choose when the task should start.
4. Click **Save**.

If no threats are found, the device will shut down.

If there remain unresolved threats, you will be prompted to choose the actions to be taken on them. For more information, refer to *“Antivirus Scan Wizard”* (p. 60).

10.4. How do I configure Bitdefender to use a proxy internet connection?

If your device 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:



1. Click **Settings** on the navigation menu on the **Bitdefender interface**.
2. Select the **Advanced** tab.
3. Turn on **Proxy server**.
4. Click **Proxy change**.
5. 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 Microsoft Edge, Internet Explorer, Mozilla Firefox and Google Chrome.

- **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.
 - **Username** - type in a user name recognized by the proxy.
 - **Password** - type in the valid password of the previously specified user.
6. 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.

10.5. 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:

- **In Windows 7:**
 1. Click **Start**.
 2. Locate **Computer** on the **Start** menu.
 3. Right-click **Computer** and select **Properties**.



4. Look under **System** to check the information about your system.

● In **Windows 8**:

1. From the Windows Start screen, locate **Computer** (for example, you can start typing "Computer" directly in the Start screen) and then right-click its icon.

In **Windows 8.1**, locate **This PC**.

2. Select **Properties** in the bottom menu.

3. Look in the System area to see your system type.

● In **Windows 10**:

1. Type "System" in the search box from the taskbar and click its icon.

2. Look in the System area to find information about your system type.

10.6. How do I display hidden objects in Windows?

These steps are useful in those cases where you are dealing with a threat 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**.

In **Windows 8 and Windows 8.1**: From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen), and then click its icon.

2. Select **Folder Options**.

3. Go to **View** tab.

4. Select **Show hidden files and folders**.

5. Clear **Hide extensions for known file types**.

6. Clear **Hide protected operating system files**.

7. Click **Apply**, then click **OK**.

In **Windows 10**:

1. Type "Show hidden files and folders" in the search box from the taskbar and click its icon.

2. Select **Show hidden files, folders, and drives**.



3. Clear **Hide extensions for known file types**.
4. Clear **Hide protected operating system files**.
5. Click **Apply**, then click **OK**.

10.7. 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 device, the system becomes unstable. The Bitdefender Antivirus Free 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:

● In **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, and then reboot your system.

● In **Windows 8 and Windows 8.1**:

1. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen), and then click its icon.
2. Click **Uninstall a program** or **Programs and Features**.
3. Wait a few moments until the installed software list is displayed.
4. Find the name of the program you want to remove and select **Uninstall**.
5. Wait for the uninstall process to complete, and then reboot your system.

● In **Windows 10**:

1. Click **Start**, then click **Settings**.
2. Click the **System** icon in the Settings area, then select **Apps**.
3. Find the name of the program you want to remove and select **Uninstall**.
4. Click **Uninstall** again to confirm your choice.



5. Wait for the uninstall process to complete, and 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 to provide you with the uninstall guidelines.

10.8. 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 threats preventing Windows from starting normally. In Safe Mode only a few apps work and Windows loads just the basic drivers and a minimum of operating system components. This is why most threats are inactive when using Windows in Safe Mode and they can be easily removed.

To start Windows in Safe Mode:

● In **Windows 7**:

1. Restart the device.
2. Press the **F8** key several times before Windows starts 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.

● In **Windows 8, Windows 8.1 and Windows 10**:

1. Launch **System Configuration** in Windows by simultaneously pressing the **Windows + R** keys on your keyboard.
2. Write **msconfig** in the **Open** dialog box, then click **OK**.
3. Select the **Boot** tab.
4. In the **Boot options** area, select the **Safe boot** check box.
5. Click **Network**, and then **OK**.



6. Click **OK** in the **System Configuration** window which informs you that the system needs to be restarted to be able to make the changes you set.

Your system is restarting in Safe Mode with Networking.

To reboot in normal mode, switch back the settings by launching again the **System Operation** and clearing the **Safe boot** check box. Click **OK**, and then **Restart**. Wait for the new settings to be applied.



MANAGING YOUR SECURITY



11. ANTIVIRUS PROTECTION

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

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

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



Important

To prevent threats from infecting your device, keep **on-access scanning** enabled.

- **On-demand scanning** - allows detecting and removing the threat 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.

Bitdefender automatically scans any removable media that is connected to the device to make sure it can be safely accessed. For more information, refer to *"Automatic scan of removable media"* (p. 64).

Advanced users can configure scan exceptions if they do not want specific files or file types to be scanned. For more information, refer to *"Configuring scan exceptions"* (p. 65).

When it detects a threat, Bitdefender will automatically attempt to remove the malicious 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 to contain the infection. For more information, refer to *"Managing quarantined files"* (p. 67).

If your device has been infected with threats, refer to *"Removing threats from your system"* (p. 86).

11.1. On-access scanning (real-time protection)

Bitdefender provides real-time protection against a wide range of threats by scanning all accessed files and email messages.



11.1.1. Turning on or off real-time protection

To turn on or off real-time protection against threats:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ANTIVIRUS** pane, click **Open**.
3. In the **Advanced** window, turn on or off **Bitdefender Shield**.
4. If you want to disable real-time protection, a warning window appears. 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 a system restart. The real-time protection will automatically turn on when the selected time will expire.



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 threats.

11.1.2. Restoring the default settings

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

To restore the default real-time protection settings:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ANTIVIRUS** pane, click **Open**.
3. In the **Advanced** window, scroll down on the window until you see the **Reset advanced settings** option. Select this option to reset the antivirus settings to default.

11.2. On-demand scanning

The main objective for Bitdefender is to keep your device clean of threats. This is done by keeping new threats out of your device and by scanning your email messages and any new files downloaded or copied to your system.

There is a risk that a threat is already lodged in your system, before you even install Bitdefender. This is why it's a very good idea to scan your device for



resident threats after you've installed Bitdefender. And it's definitely a good idea to frequently scan your device for threats.

On-demand scanning is based on scan tasks. Scan tasks specify the scanning options and the objects to be scanned. You can scan the device 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 device or to configure the scan options, configure and run a custom scan.

11.2.1. Scanning a file or folder for threats

You should scan files and folders whenever you suspect they might be infected. Right-click the file or folder you want to be scanned, point to **Bitdefender** and select **Scan with Bitdefender**. The **Antivirus Scan wizard** will appear and guide you through the scanning process. At the end of the scan, you will be prompted to choose the actions to be taken on the detected files, if any.

11.2.2. Running a Quick Scan

Quick Scan uses in-the-cloud scanning to detect threats 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 antivirus scan.

To run a Quick Scan:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ANTIVIRUS** pane, click **Open**.
3. In the **Scans** windows, click the **Run Scan** button next to **Quick Scan**.
4. Follow the **Antivirus Scan wizard** to complete the scan. Bitdefender will automatically take the recommended actions on detected files. If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

11.2.3. Running a System Scan

The System Scan task scans the entire device for all types of threats endangering its security, such as malware, spyware, adware, rootkits and others.



Note

Because **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 device.

Before running a System Scan, the following are recommended:

- Make sure Bitdefender is up-to-date with its threat information database. Scanning your device using an outdated threat information database may prevent Bitdefender from detecting new threats found since the last update. For more information, refer to *“Keeping Bitdefender up-to-date”* (p. 28).
- Shut down all open programs.

If you want to scan specific locations on your device or to configure the scanning options, configure and run a custom scan. For more information, refer to *“Configuring a custom scan”* (p. 57).

To run a System Scan:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ANTIVIRUS** pane, click **Open**.
3. In the **Scans** windows, click the **Run Scan** button next to **System Scan**.
4. The first time you run a System Scan, you are introduced into the feature. Click **Ok, got it** to continue.
5. Follow the **Antivirus Scan wizard** to complete the scan. Bitdefender will automatically take the recommended actions on detected files. If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

11.2.4. Configuring a custom scan

In the **Manage Scans** window, you can set up Bitdefender to run scans whenever you consider that your device needs a check for potential threats. You can choose to schedule a **System Scan** or a **Quick Scan**, or you can create a custom scan at your convenience.

To configure a new custom scan in detail:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ANTIVIRUS** pane, click **Open**.
3. In the **Scans** windows, click **+Create scan**.



4. In the **Task Name** field, type a name for the scan, then select the locations you would like to be scanned, and then click **Next**.
5. Configure these general options:
 - **Scan only applications.** You can set Bitdefender to scan only accessed apps.
 - **Scan task priority.** You can choose the impact a scan process should have on your system performance.
 - **Auto** - The priority of the scan process will depend on the system activity. To make sure that the scan process will not affect the system activity, Bitdefender will decide whether the scan process should be run with high or low priority.
 - **High** - The priority of the scan process will be high. By choosing this option, you will allow other programs to run slower and decrease the time needed for the scan process to finish.
 - **Low** - The priority of the scan process will be low. By choosing this option, you will allow other programs to run faster and increase the time needed for the scan process to finish.
 - **Post scan actions.** Choose what action Bitdefender should take in case no threats are found:
 - Show Summary window
 - Shutdown device
 - Close Scan window
6. If you want to configure the scanning options in detail, click **Show advanced options**. You can find information about the listed scans at the end of this section.
Click **Next**.
7. You can enable **Schedule scan task** if you wish, and then choose when the custom scan you created should start.
 - At system startup
 - Daily
 - Monthly
 - Weekly



If you choose Daily, Monthly, or Weekly, drag the slider along the scale to set the desired period of time when the scheduled scan should start.

8. Click **Save** to save the settings and close the configuration window.

Depending on the locations to be scanned, the scan may take a while. If threats will be found during the scanning process, you will be prompted to choose the actions to be taken on the detected files.

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 potentially unwanted applications.** Select this option to scan for unwanted applications. A potentially unwanted application (PUA) or potentially unwanted program (PUP) is a software that usually comes bundled with freeware software and will display pop-ups or install a toolbar in the default browser. Some of them will change the homepage or the search engine, others will run several processes in the background slowing down the PC or will display numerous ads. These programs can be installed without your consent (also called adware) or will be included by default in the express installation kit (ad-supported).
- **Scan archives.** Archives containing infected files are not an immediate threat to the security of your system. The threat 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 to detect and remove any potential threat, even if it is not an immediate threat.

Drag the slider along the scale to exclude from scanning archives that are bigger than a given value in MB (Megabytes).



Note

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

- **Scan only new and modified files.** By scanning only new and modified files, you may greatly improve overall system responsiveness with a minimum trade-off in security.




- **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 threat 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 apps.
- **Scan cookies.** Select this option to scan the cookies stored by browsers on your device.
- **Scan keyloggers.** Select this option to scan your system for keylogger apps. Keyloggers record what you type on your keyboard and send reports over the internet to a malicious person (hacker). The hacker can find out sensitive information from the stolen data, such as bank account numbers and passwords, and use it to gain personal benefits.

11.2.5. Antivirus Scan Wizard

Whenever you initiate an on-demand scan (for example, right-click a folder, point to Bitdefender 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  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 - Perform scan

Bitdefender will start scanning the selected objects. You can see real-time information about the scan status and statistics (including the elapsed time, an estimation of the remaining time and the number of detected threats).

Wait for Bitdefender to finish scanning. The scanning process may take a while, depending on the complexity of the scan.



Stopping or pausing the scan. You can stop scanning anytime you want by clicking **STOP**. 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.

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:

- **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 item from scan.** 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.

Choose the desired option and click **OK** to continue scanning.

Step 2 - Choose actions

At the end of the scan, you will be prompted to choose the actions to be taken on the detected files, if any.



Note

When you run a quick scan or a system scan, Bitdefender will automatically take the recommended actions on detected files during the scan. If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

The infected objects are displayed in groups, based on the threats 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 proper actions

Bitdefender will take the recommended actions depending on the type of detected file:

- **Infected files.** Files detected as infected match a piece of threat information found in the Bitdefender Threat Information Database. Bitdefender will automatically attempt to remove the malicious 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 to contain the infection. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. For more information, refer to "*Managing quarantined files*" (p. 67).



Important

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

- **Suspicious files.** Files are detected as suspicious by the heuristic analysis. Suspicious files cannot be disinfected, because no disinfection routine is available. They will be moved to quarantine to prevent a potential infection.

By default, quarantined files are automatically sent to Bitdefender Labs to be analyzed by the Bitdefender threat researchers. If a threat presence is confirmed, an information update is released to allow removing the threat.

- **Archives containing infected files.**

- Archives that contain only infected files are deleted automatically.
- If an archive contains both infected and clean files, Bitdefender will attempt to delete the infected files provided it can reconstruct the archive with the clean files. If archive reconstruction is not possible, you will be informed that no action can be taken so as to avoid losing clean files.

Delete

Removes detected files from the disk.



If infected files are stored in an archive together with clean files, Bitdefender will attempt to delete the infected files and reconstruct the archive with the clean files. If archive reconstruction is not possible, you will be informed that no action can be taken so as to avoid losing clean files.

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.

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

Step 3 - 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

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. If required, restart your system to complete the cleaning process. For more information and instructions on how to remove a threat manually, refer to *"Removing threats from your system"* (p. 86).

11.2.6. Checking scan logs

Each time a scan is performed, a scan log is created and Bitdefender records the detected issues in the Antivirus window. 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 a scan log or any detected infection at a later time:

1. Click **Notifications** on the navigation menu on the **Bitdefender interface**.
2. In the **All** tab, select the notification regarding the latest scan.

This is where you can find all threat scan events, including threats detected by on-access scanning, user-initiated scans and status changes for automatic scans.



3. In the notifications list, you can check what scans have been performed recently. Click a notification to view details about it.
4. To open the scan log, click **View log**.

11.3. Automatic scan of removable media

Bitdefender automatically detects when you connect a removable storage device to your device and scans it in the background when the Autoscan option is enabled. This is recommended to prevent threats from infecting your device.


Detected devices fall into one of these categories:

- CDs/DVDs
- Flash drives, 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.

11.3.1. How does it work?

When it detects a removable storage device, Bitdefender starts scanning it for threats (provided automatic scan is enabled for that type of device). You will be notified through a pop-up window that a new device has been detected and it is being scanned.

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.

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

In most cases, Bitdefender automatically removes detected threats 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.

This information may be useful to you:



- Be careful when using a threat-infected CD/DVD, because the threat cannot be removed from the disc (the media is read-only). Make sure real-time protection is turned on to prevent threats 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 threats 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 threats, refer to *"Removing threats from your system"* (p. 86).

11.3.2. Managing removable media scan

To manage automatic scan of removable media:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ANTIVIRUS** pane, click **Open**.
3. Select the **Settings** window.

The scanning options are pre-configured for the best detection results. If infected files are detected, Bitdefender will try to disinfect them (remove the malicious 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.

For best protection, it is recommended to let selected the **Autoscan** option for all types of removable storage devices.

11.4. Configuring scan exceptions

Bitdefender allows excepting 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. Exceptions are to be used by users having advanced computer knowledge or, otherwise, following the recommendations of a Bitdefender representative.

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



Note

Exceptions 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**.

11.4.1. Excepting files and folders from scanning

To except specific files and folders from scanning:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ANTIVIRUS** pane, click **Open**.
3. In the **Settings** window, click **Manage Exceptions**.
4. Click **+Add an Exception**.
5. Enter the path of the folder you want to except from scanning in the corresponding field.

Alternatively, you can navigate to the folder by clicking the browse button in the right side of the interface, select it and click on **OK**.

6. Turn on the switch next to the protection feature that should not scan the folder. There are three options:
 - Antivirus
 - Online Threat Prevention
 - Advanced Threat Defense
7. Click **Save** to save the changes and close the window.

11.4.2. Excepting file extensions from scanning

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



Important

Use caution when excepting extensions from scanning because such exceptions can make your device vulnerable to threats.

To except file extensions from scanning:




1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ANTIVIRUS** pane, click **Open**.
3. In the **Settings** window, click **Manage Exceptions**.
4. Click **+Add an Exception**.
5. Type the extensions that you want to be excepted from scanning with a dot before them, separating them with semicolons (;).
txt;avi;jpg
6. Turn on the switch next to the protection feature that should not scan the extension.
7. Click **Save**.

11.4.3. Managing scan exceptions

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

To manage scan exceptions:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ANTIVIRUS** pane, click **Open**.
3. In the **Settings** window, click **Manage Exceptions**. A list with all your exceptions will be displayed.
4. To remove or edit scan exceptions, click one of the available buttons. Proceed as follows:

- To remove an entry from the list, click the  button next to it.
- To edit an entry from the table, click the **Edit** button next to it. A new window appears where you can change the extension or the path to be excepted and the security feature you want them to be excepted from, as needed. Make the necessary changes, then click **MODIFY**.

11.5. Managing quarantined files

Bitdefender isolates the threat-infected files it cannot disinfect and the suspicious files in a secure area named quarantine. When a threat 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 to be analyzed by the Bitdefender threat researchers. If a threat presence is confirmed, an information update is released to allow removing the threat.

In addition, Bitdefender scans the quarantined files each time the threat information database is updated. Cleaned files are automatically moved back to their original location.

To check and manage quarantined files:

1. Click **Protection** on the navigation menu on the [Bitdefender interface](#).
2. In the **ANTIVIRUS** pane, click **Open**.
3. Go to the **Settings** window.

Here you can view the name of the quarantined files, their original location and the name of the detected threats.

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 by clicking **View Settings**.

Click the switches to turn on or off:

Rescan quarantine after threat information update

Keep this option turned on to automatically scan quarantined files after each threat information database is updated. Cleaned files are automatically moved back to their original location.

Delete content older than 30 days

Quarantined files older than 30 days are automatically deleted.

Create exceptions for restored files

The files you restore from quarantine are moved back to their original location without being repaired and automatically excepted from future scans.

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**.



12. ADVANCED THREAT DEFENSE

Bitdefender Advanced Threat Defense is an innovative proactive detection technology which uses advanced heuristic methods to detect ransomware and other new potential threats in real time.

Advanced Threat Defense continuously monitors the apps running on the device, looking for threat-like actions. Each of these actions is scored and an overall score is computed for each process.

As a safety measure you will be notified each time threats and potentially malicious processes are detected and blocked.

12.1. Turning on or off Advanced Threat Defense

To turn on or off Advanced Threat Defense:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ADVANCED THREAT DEFENSE** pane, click **Open**.
3. Go to the **Settings** window and click switch next to **Bitdefender Advanced Threat Defense**.



Note

To keep your system protected from ransomware and other threats, we recommend you to disable Advanced Threat Defense for as little time as possible.

12.2. Checking detected malicious attacks

Whenever threats or potentially malicious processes are detected, Bitdefender will block them to prevent your device from being infected by ransomware or other malware. You can check at any time the list of detected malicious attacks by following these steps:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ADVANCED THREAT DEFENSE** pane, click **Open**.
3. Go to the **Threat Defense** window.

The attacks detected in the latest 90 days are displayed. To find details about the type of a detected ransomware, the path of the malicious process, or if the disinfection has been successful, simply click it.



12.3. Adding processes to exceptions

You can configure exception rules for trusted apps so that Advanced Threat Defense does not block them if they perform threat-like actions.

To start adding processes to the Advanced Threat Defense exceptions list:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ADVANCED THREAT DEFENSE** pane, click **Open**.
3. In the **Settings** window, click **Manage Exceptions**.
4. Click **+Add an Exception**.
5. Enter the path of the folder you want to except from scanning in the corresponding field.

Alternatively, you can navigate to the executable by clicking the browse button in the right side of the interface, select it and click on **OK**.

6. Turn on the switch next to **Advanced Threat Defense**.
7. Click **Save**.

12.4. Exploits detection

A way used by hackers to breach systems, is to take advantage of particular bugs or vulnerabilities present in computer software (apps or plugins) and hardware. To make sure that your device stays away from such attacks, that normally spread very fast, Bitdefender uses the newest anti-exploit technologies.

Turning on or off exploit detection

To turn on or off the exploit detection:

- Click **Protection** on the navigation menu on the **Bitdefender interface**.
- In the **ADVANCED THREAT DEFENSE** pane, click **Open**.
- Go to the **Settings** window and click the switch next to **Exploit detection** to turn the feature on or off.



Note

The Exploit detection option is enabled by default.



13. ONLINE THREAT PREVENTION

Bitdefender Online Threat Prevention ensures a safe browsing experience by alerting you about potential malicious webpages.

Bitdefender provides real-time online threat prevention for:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

To configure Online Threat Prevention settings:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ONLINE THREAT PREVENTION** pane, click **Settings**.

In the **Web Protection** sections, click the switches to turn on or off:

- Web attack prevention blocks threats coming from the internet, including drive-by downloads.
- Search Advisor, a component that rates the results of your search engine queries and the links posted on social networking websites by placing an icon next to every result:
 - You should not visit this webpage.
 - ⚠ This webpage may contain dangerous content. Exercise caution if you decide to visit it.
 - ✔ This is a safe page to visit.

Search Advisor rates the search results from the following web search engines:

- Google
- Yahoo!
- Bing
- Baidu

Search Advisor rates the links posted on the following online social networking services:




- Facebook
- Twitter
- Encrypted web scan.

More sophisticated attacks might use secure web traffic to mislead their victims. Therefore, we recommend you to keep enabled the Encrypted web scan option.

- Fraud protection.
- Phishing protection.

You can create a list of websites, domains, and IP addresses that will not be scanned by the Bitdefender anti-threat, antiphishing, and antifraud engines. The list should contain only websites, domains, and IP addresses that you fully trust.

To configure and manage websites, domains, and IP addresses using the Online Threat Prevention feature provided by Bitdefender:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ONLINE THREAT PREVENTION** pane, click **Settings**.
3. Click **Manage exceptions**.
4. Click **+Add an Exception**.
5. Type in the corresponding field the name of the website, the name of the domain, or the IP address you want to add to exceptions.
6. Click the switch next to **Online Threat Prevention**.
7. To remove an entry from the list, click the  button next to it.
Click **Save** to save the changes and close the window.

13.1. 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 website by clicking **TAKE ME BACK TO SAFETY**.



- Proceed to the website, despite the warning, by clicking **I understand the risks, take me there anyway**.
- If you are sure that the detected website is safe, click **SUBMIT** to add it to exceptions. We recommend you to add only websites that you fully trust.



TROUBLESHOOTING



14. SOLVING COMMON ISSUES

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. 75)
- *“Scan doesn’t start”* (p. 76)
- *“I can no longer use an app”* (p. 79)
- *“What to do when Bitdefender blocks a website, a domain, an IP address, or an online app that are safe”* (p. 80)
- *“How to update Bitdefender on a slow internet connection”* (p. 80)
- *“Bitdefender services are not responding”* (p. 81)
- ???
- *“Bitdefender removal failed”* (p. 82)
- *“My system doesn’t boot up after installing Bitdefender”* (p. 83)

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 *“Asking for help”* (p. 93).

14.1. 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 slowdown, 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 security solution you may use before installing Bitdefender. For more information, refer to *“How do I remove other security solutions?”* (p. 50).

- **The system requirements for running Bitdefender are not met.**



If your machine does not meet the system requirements, the device will become sluggish, especially when multiple apps are running at the same time. For more information, refer to "[System requirements](#)" (p. 3).

- **You have installed apps that you do not use.**

Any device has programs or apps that you do not use. And many unwanted programs run in the background taking up disk space and memory. If you do not use a program, uninstall it. This is also valid for any other pre-installed software or trial app you forgot to remove.



Important

If you suspect a program or an app to be an essential part of your operating system, do not remove it and contact Bitdefender Customer Care for assistance.

- **Your system may be infected.**

Your system speed and its general behavior can also be affected by threats. Spyware, malware, Trojans and adware all take a toll on your device's performance. Make sure to scan your system periodically, at least once a week. It is recommended to use the Bitdefender System Scan because it scans for all types of threats endangering the security of your system.

To start the System Scan:

1. Click **Protection** on the navigation menu on the [Bitdefender interface](#).
2. In the **ANTIVIRUS** pane, click **Open**.
3. In the **Scans** window, click **Run Scan** next to **System Scan**.
4. Follow the wizard steps.

14.2. 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 reinstall Bitdefender:

- **In Windows 7:**

1. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.



2. Find **Bitdefender Antivirus Free** and select **Uninstall**.
 3. Click **REINSTALL** in the window that appears.
 4. Wait for the reinstall process to complete, and then reboot your system.
- In **Windows 8 and Windows 8.1**:
 1. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen), and then click its icon.
 2. Click **Uninstall a program** or **Programs and Features**.
 3. Find **Bitdefender Antivirus Free** and select **Uninstall**.
 4. Click **REINSTALL** in the window that appears.
 5. Wait for the reinstall process to complete, and then reboot your system.
 - In **Windows 10**:
 1. Click **Start**, then click Settings.
 2. Click the **System** icon in the Settings area, then select **Installed apps**.
 3. Find **Bitdefender Antivirus Free** and select **Uninstall**.
 4. Click **Uninstall** again to confirm your choice.
 5. Click **REINSTALL** in the window that appears.
 6. Wait for the reinstall process to complete, and then reboot your system.



Note

By following this reinstall procedure, customized settings are saved and available in the new installed product. Other settings may be switched back to their default configuration.

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

In this case:

1. Remove the other security solution. For more information, refer to *"How do I remove other security solutions?"* (p. 50).
2. Reinstall Bitdefender:



- In **Windows 7**:
 - a. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
 - b. Find **Bitdefender Antivirus Free** and select **Uninstall**.
 - c. Click **REINSTALL** in the window that appears.
 - d. Wait for the reinstall process to complete, and then reboot your system.
- In **Windows 8 and Windows 8.1**:
 - a. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen), and then click its icon.
 - b. Click **Uninstall a program** or **Programs and Features**.
 - c. Find **Bitdefender Antivirus Free** and select **Uninstall**.
 - d. Click **REINSTALL** in the window that appears.
 - e. Wait for the reinstall process to complete, and then reboot your system.
- In **Windows 10**:
 - a. Click **Start**, then click **Settings**.
 - b. Click the **System** icon in the Settings area, then select **Installed apps**.
 - c. Find **Bitdefender Antivirus Free** and select **Uninstall**.
 - d. Click **Uninstall** again to confirm your choice.
 - e. Click **REINSTALL** in the window that appears.
 - f. Wait for the reinstall process to complete, and then reboot your system.



Note

By following this reinstall procedure, customized settings are saved and available in the new installed product. Other settings may be switched back to their default configuration.

If this information was not helpful, you can contact Bitdefender for support as described in section *"Asking for help"* (p. 93).



14.3. I can no longer use an app

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

After 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 Advanced Threat Defense mistakenly detects some apps as malicious.

Advanced Threat Defense is a Bitdefender feature which constantly monitors the apps 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 apps are reported by Advanced Threat Defense.

When this situation occurs, you can except the respective app from being monitored by Advanced Threat Defense.

To add the program to the exceptions list:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ADVANCED THREAT DEFENSE** pane, click **Open**.
3. In the **Settings** window, click **Manage Exceptions**.
4. Click **+Add an Exception**.
5. Enter the path of the executable you want to except from scanning in the corresponding field.

Alternatively, you can navigate to the executable by clicking the browse button in the right side of the interface, select it and click on **OK**.

6. Turn on the switch next to **Advanced Threat Defense**.
7. Click **Save**.

If this information was not helpful, you can contact Bitdefender for support as described in section *"Asking for help"* (p. 93).



14.4. What to do when Bitdefender blocks a website, a domain, an IP address, or an online app that are safe

Bitdefender offers a secure web browsing experience by filtering all web traffic and blocking any malicious content. However, it is possible that Bitdefender considers a website, a domain, an IP address, or online app that are safe as unsafe, which will cause Bitdefender HTTP traffic scanning to block them incorrectly.

Should the same page, domain, IP address, or online app be blocked repeatedly, they can be added to exceptions so that they will not be scanned by the Bitdefender engines, thus ensuring a smooth web browsing experience.

To add a website to **Exceptions**:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. In the **ONLINE THREAT PREVENTION** pane, click **Settings**.
3. Click **Manage exceptions**.
4. Click **+Add an Exception**.
5. Type in the corresponding field the name of the website, the name of the domain, or the IP address you want to add to exceptions.
6. Click the switch next to **Online Threat Prevention**.
7. Click **Save** to save the changes and close the window.

Only websites, domains, IP addresses, and apps that you fully trust should be added to this list. These will be excepted from scanning by the following engines: threat, phishing and fraud.

If this information was not helpful, you can contact Bitdefender for support as described in section *"Asking for help"* (p. 93).

14.5. 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 threat information database:

1. Click **Settings** on the navigation menu on the **Bitdefender interface**.



2. Select the **Update** tab.
3. Turn off the **Silent update** switch.
4. Next time when an update will be available, you will be prompted to select which update you would like to download. Select only **Signatures update**.
5. Bitdefender will download and install only the threat information database.

14.6. 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:

- temporary communication errors between the Bitdefender services.
- some of the Bitdefender services are stopped.
- other security solutions running on your device 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 device and wait a few moments until Bitdefender is loaded. Open Bitdefender to see if the error persists. Restarting the device 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, refer to *"How do I remove other security solutions?"* (p. 50).

If the error persists, please contact our support representatives for help as described in section *"Asking for help"* (p. 93).



14.7. Bitdefender removal failed

If you want to remove your Bitdefender product and you notice that the process hangs out or the system freezes, click **Cancel** to abort the action. If this does not work, restart the system.

When 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.

To completely remove Bitdefender from your system:

● In Windows 7:

1. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
2. Find **Bitdefender Antivirus Free** and select **Uninstall**.
3. Click **REMOVE** in the window that appears.
4. Wait for the uninstall process to complete, and then reboot your system.

● In Windows 8 and Windows 8.1:

1. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen), and then click its icon.
2. Click **Uninstall a program** or **Programs and Features**.
3. Find **Bitdefender Antivirus Free** and select **Uninstall**.
4. Click **REMOVE** in the window that appears.
5. Wait for the uninstall process to complete, and then reboot your system.

● In Windows 10:

1. Click **Start**, then click **Settings**.
2. Click the **System** icon in the Settings area, then select **Installed apps**.
3. Find **Bitdefender Antivirus Free** and select **Uninstall**.
4. Click **Uninstall** again to confirm your choice.
5. Click **REMOVE** in the window that appears.
6. Wait for the uninstall process to complete, and then reboot your system.



14.8. 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:

1. Reboot your system and enter in Safe Mode. To find out how to do this, refer to *"How do I restart in Safe Mode?"* (p. 51).
2. Remove Bitdefender from your system:

● In Windows 7:

- a. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
- b. Find **Bitdefender Antivirus Free** and select **Uninstall**.
- c. Click **REMOVE** in the window that appears.
- d. Wait for the uninstall process to complete, and then reboot your system.
- e. Reboot your system in normal mode.

● In Windows 8 and Windows 8.1:

- a. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen), and then click its icon.
- b. Click **Uninstall a program** or **Programs and Features**.
- c. Find **Bitdefender Antivirus Free** and select **Uninstall**.
- d. Click **REMOVE** in the window that appears.
- e. Wait for the uninstall process to complete, and then reboot your system.



f. Reboot your system in normal mode.

● In **Windows 10**:

a. Click **Start**, then click Settings.

b. Click the **System** icon in the Settings area, then select **Installed apps**.

c. Find **Bitdefender Antivirus Free** and select **Uninstall**.

d. Click **Uninstall** again to confirm your choice.

e. Click **REMOVE** in the window that appears.

f. Wait for the uninstall process to complete, and then reboot your system.

g. Reboot your system in normal mode.

3. Reinstall your Bitdefender product.

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

To solve this:

1. Reboot your system and enter in Safe Mode. To find out how to do this, refer to *"How do I restart in Safe Mode?"* (p. 51).

2. Remove the other security solution from your system:

● In **Windows 7**:

a. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.

b. Find the name of the program you want to remove and select **Remove**.

c. Wait for the uninstall process to complete, and then reboot your system.

● In **Windows 8 and Windows 8.1**:

a. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen), and then click its icon.

b. Click **Uninstall a program** or **Programs and Features**.



- c. Find the name of the program you want to remove and select **Remove**.
 - d. Wait for the uninstall process to complete, and then reboot your system.
- In **Windows 10**:
- a. Click **Start**, then click Settings.
 - b. Click the **System** icon in the Settings area, then select **Installed apps**.
 - c. Find the name of the program you want to remove and select **Uninstall**.
 - d. Wait for the uninstall process to complete, and then reboot your system.

To correctly uninstall the other software, go to their website and run their uninstall tool or contact them directly to provide you with the uninstall guidelines.

3. 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:

1. Reboot your system and enter in Safe Mode. To find out how to do this, refer to *"How do I restart in Safe Mode?"* (p. 51).
2. Use the System Restore option from Windows to restore the device to an earlier date before installing the Bitdefender product.
3. Reboot the system in normal mode and contact our support representatives for help as described in section *"Asking for help"* (p. 93).



15. REMOVING THREATS FROM YOUR SYSTEM

Threats can affect your system in many different ways and the Bitdefender approach depends on the type of threat attack. Because threats 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 threat infection from your system. In such cases, your intervention is required.

- ???
- *"What to do when Bitdefender finds threats on your device?"* (p. 86)
- *"How do I clean a threat in an archive?"* (p. 87)
- *"How do I clean a threat in an email archive?"* (p. 89)
- *"What to do if I suspect a file as being dangerous?"* (p. 89)
- *"What are the password-protected files in the scan log?"* (p. 90)
- *"What are the skipped items in the scan log?"* (p. 90)
- *"What are the over-compressed files in the scan log?"* (p. 91)
- *"Why did Bitdefender automatically delete an infected file?"* (p. 91)

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 *"Asking for help"* (p. 93).

15.1. What to do when Bitdefender finds threats on your device?

You may find out there is a threat on your device in one of these ways:

- You scanned your device and Bitdefender found infected items on it.
- A threat alert informs you that Bitdefender blocked one or multiple threats on your device.

In such situations, update Bitdefender to make sure you have the latest threat information database and run a System Scan to analyze the system.

As soon as the system 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. Click **Protection** on the navigation menu on the **Bitdefender interface**.
 - b. In the **ANTIVIRUS** pane, click **Open**.
 - c. In the **Advanced** window, turn off **Bitdefender Shield**.
2. Display hidden objects in Windows. To find out how to do this, refer to *"How do I display hidden objects in Windows?"* (p. 49).
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:

1. Reboot your system and enter in Safe Mode. To find out how to do this, refer to *"How do I restart in Safe Mode?"* (p. 51).
2. Display hidden objects in Windows. To find out how to do this, refer to *"How do I display hidden objects in Windows?"* (p. 49).
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. 93).

15.2. How do I clean a threat 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 threats inside them, but is not able to take any other actions.

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

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

1. Identify the archive that includes the threat by performing a System Scan of the system.
2. Turn off the Bitdefender real-time antivirus protection:
 - a. Click **Protection** on the navigation menu on the **Bitdefender interface**.
 - b. In the **ANTIVIRUS** pane, click **Open**.
 - c. In the **Advanced** window, turn off **Bitdefender Shield**.
3. Go to the location of the archive and decompress it using an archiving app, like WinZip.
4. Identify the infected file and delete it.
5. Delete the original archive to make sure the infection is totally removed.
6. Recompress the files in a new archive using an archiving app, like WinZip.
7. Turn on the Bitdefender real-time antivirus protection and run a System scan to make sure there is no other infection on the system.



Note

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

If this information was not helpful, you can contact Bitdefender for support as described in section *"Asking for help"* (p. 93).



15.3. How do I clean a threat in an email archive?

Bitdefender can also identify threats in email databases and email 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 threat stored in an email archive:

1. Scan the email database with Bitdefender.
2. Turn off the Bitdefender real-time antivirus protection:
 - a. Click **Protection** on the navigation menu on the **Bitdefender interface**.
 - b. In the **ANTIVIRUS** pane, click **Open**.
 - c. In the **Advanced** window, turn off **Bitdefender Shield**.
3. Open the scan report and use the identification information (Subject, From, To) of the infected messages to locate them in the email client.
4. Delete the infected messages. Most email 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 Microsoft Outlook 2007: On the File menu, click Data File Management. Select the personal folders (.pst) files you intend to compact, and click Settings. Click Compact Now.
 - In Microsoft Outlook 2010 / 2013/ 2016: On the File menu, click Info, and then Account settings (Add and remove accounts or change existing connection settings). Then click Data File, select the personal folders (.pst) files you intend to compact, and click Settings. Click Compact Now.
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. 93).

15.4. 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:

1. Run a **System Scan** with Bitdefender. To find out how to do this, refer to *"How do I scan my system?"* (p. 39).
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, refer to *"Asking for help"* (p. 93).

15.5. 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.

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 device protected. If you want to scan those files with Bitdefender, you have to contact the product manufacturer 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.

15.6. 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.



15.7. 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.

15.8. 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 to contain the infection.

For particular types of threats, 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.



CONTACT US



16. ASKING FOR HELP

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

The *“Solving common issues”* (p. 75) section provides the necessary information regarding the most frequent issues you may encounter when using this product.

If you do not find an answer to your question in the provided resources, you can contact us directly:

- *“Contact us directly from Bitdefender Antivirus Free”* (p. 93)
- *“Contact us through our online Support Center”* (p. 94)

Contact us directly from Bitdefender Antivirus Free

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

Follow these steps:

1. Click the **Support** button, represented by a **question mark**, in the upper part of the **Bitdefender interface**.
2. You have the following options:

- **USER'S GUIDE**

Access our database and search for the necessary information.

- **SUPPORT CENTER**

Access our online articles and video tutorials.

- **ASK THE COMMUNITY**

Click **ASK THE COMMUNITY** to access the Bitdefender community where you can get answers and guidance from other Bitdefender users.



Contact us through our online Support Center

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

1. Go to <https://www.bitdefender.com/support/consumer.html>.

The Bitdefender Support Center hosts numerous articles that contain solutions to Bitdefender-related issues.

2. Use the search bar at the top of the window to find articles that may provide a solution to your problem. To search, just type a term in the Search bar and click **Search**.
3. Read the relevant articles or documents and try the proposed solutions.
4. If the solution does not solve your problem, go to

<https://www.bitdefender.com/support/contact-us.html> and contact our support representatives.



17. ONLINE RESOURCES

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

- Bitdefender Support Center:

<https://www.bitdefender.com/support/consumer.html>

- Bitdefender Support Forum:

<https://forum.bitdefender.com>

- The HOTforSecurity computer security portal:

<https://www.hotforsecurity.com>

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

17.1. 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 threat 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

<https://www.bitdefender.com/support/consumer.html>.

17.2. 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 threats from your device 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 to assist you. You may also get an answer or a solution from a more experienced Bitdefender user.

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

The Bitdefender Support Forum is available at <https://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.

17.3. HOTforSecurity Portal

HOTforSecurity is a rich source of computer security information. Here you can learn about the various threats your device is exposed to when connected to the internet (malware, phishing, spam, cyber-criminals).

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 HOTforSecurity webpage is <https://www.hotforsecurity.com>.



18. CONTACT INFORMATION

Efficient communication is the key to a successful business. Since 2001 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.

18.1. Web addresses

Sales department: sales@bitdefender.com
Support Center: <https://www.bitdefender.com/support/consumer.html>
Documentation: documentation@bitdefender.com
Local distributors: <https://www.bitdefender.com/partners>
Partner program: partners@bitdefender.com
Media relations: pr@bitdefender.com
Careers: jobs@bitdefender.com
Threat submissions: virus_submission@bitdefender.com
Spam submissions: spam_submission@bitdefender.com
Report abuse: abuse@bitdefender.com
Website: <https://www.bitdefender.com>

18.2. 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 <https://www.bitdefender.com/partners/partner-locator.html>.
2. Choose your country and city using the corresponding options.
3. If you do not find a Bitdefender distributor in your country, feel free to contact us by email at sales@bitdefender.com. Write your email in English in order for us to be able to assist you promptly.

18.3. 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

6301 NW 5th Way, Suite 4300

Fort Lauderdale, Florida 33309

Phone (office&sales): 1-954-776-6262

Sales: sales@bitdefender.com

Technical support: <https://www.bitdefender.com/support/consumer.html>

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

UK and Ireland

BITDEFENDER LTD

C/O Howsons Winton House, Stoke Road, Stoke on Trent

Staffordshire, United Kindon, ST4 2RW

Email: info@bitdefender.co.uk

Phone: (+44) 2036 080 456

Sales: sales@bitdefender.co.uk

Technical support: <https://www.bitdefender.co.uk/support/>

Web: <https://www.bitdefender.co.uk>

Germany

Bitdefender GmbH

TechnoPark Schwerte

Lohbachstrasse 12

D - 58239 Schwerte

Office: +49 2304 9 45 - 162

Fax: +49 2304 9 45 - 169

Sales: vertrieb@bitdefender.de

Technical support: <https://www.bitdefender.de/support/consumer.html>

Web: <https://www.bitdefender.de>

Denmark

Bitdefender APS

Agern Alle 24, 2970 Hørsholm, Denmark

Office: +45 7020 2282

Technical support: <http://bitdefender-antivirus.dk/>

Web: <http://bitdefender-antivirus.dk/>



Spain

Bitdefender España, S.L.U.

C/Bailén, 7, 3-D

08010 Barcelona

Fax: +34 93 217 91 28

Phone: +34 902 19 07 65

Sales: comercial@bitdefender.es

Technical support: <https://www.bitdefender.es/support/consumer.html>

Website: <https://www.bitdefender.es>

Romania

BITDEFENDER SRL

Orhideea Towers Building, 15A Orhideelor Street, 11th floor, district 6

Bucharest

Fax: +40 21 2641799

Sales phone: +40 21 2063470

Sales email: sales@bitdefender.ro

Technical support: <https://www.bitdefender.ro/support/consumer.html>

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

United Arab Emirates

Dubai Internet City

Building 17, Office # 160

Dubai, UAE

Sales phone: 00971-4-4588935 / 00971-4-4589186

Sales email: mena-sales@bitdefender.com

Technical support: <https://www.bitdefender.com/support/consumer.html>

Website: <https://www.bitdefender.com>



Glossary

Activation code

Is a unique key that can be bought from retail and used to activate a specific product or service. An activation code enables the activation of a valid subscription for a certain period of time and number devices and can also be used to extend a subscription with the condition to be generated for the same product or service.

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 webpages 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 webpage. 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.

Advanced persistent threat

Advanced persistent threat (APT) exploits vulnerabilities of systems to steal important information to deliver it to the source. Big groups such as organizations, companies, or governments, are targeted by this threat.

The objective of an advanced persistent threat is to remain undetected for a long time being able to monitor and gather important information without damaging the targeted machines. The method used to inject the threat into the network is through a PDF file or an Office document that look harmless so that every user can run the files.

Adware

Adware is often combined with a host app that is provided at no charge as long as the user agrees to accept the adware. Because adware apps are usually installed after the user has agreed to a licensing agreement that states the purpose of the app, 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 apps 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 threat 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 threat to become active in memory. Every time you boot your system from that point on, you will have the threat active in memory.

Botnet

The term "botnet" is composed of the words "robot" and "network". Botnets are internet-connected devices infected with threats and can be used to send spam emails, steal data, remotely control vulnerable devices, or spread spyware, ransomware, and other kinds of threats. Their objective is to infect as many connected devices as possible, such as PCs, servers, mobile or IoT devices belonging to big companies or industries.

Browser

Short for web browser, a software app used to locate and display webpages. Popular browsers include Microsoft Internet Explorer, Mozilla Firefox and Google Chrome. 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.

Brute Force Attack

Password guessing attack used to break into a computer system by entering possible password combinations, mostly starting with the easiest-to-guess password.

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.

Cyberbullying

When peers or strangers are committing abusive acts against children on purpose to physically hurt them. To damage emotionally, the assaulters are sending mean messages or unflattering photos, thus making their victims isolate from others or feel frustrated.

Dictionary Attack

Password guessing attacks used to break into a computer system by entering a combination of common words to generate potential passwords. The same method is used to guess decryption keys of encrypted messages or documents. Dictionary attacks succeed because many people incline to choose short and single words passwords that are easy to be guessed.



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.

Email

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.

Exploits

A way to take advantage of different bugs or vulnerabilities that are present in a computer (software or hardware). Thus, hackers may gain the control of computers or networks.

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 threats. This method of scanning does not rely on specific threat information database. The advantage of the heuristic scan is that it is not fooled by a new variant of an existing threat. However, it might occasionally report suspicious code in normal programs, generating the so-called "false positive".

Honeypot

A decoy computer system set to attract hackers to study the way they act and identify the heretical methods they use to collect system information. Companies and corporations are more interested in implementing and using honeypots to improve their overall state of security.

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 webpage. To use an applet on a webpage, you would specify the name of the applet and the size (length and width, in pixels) that the applet can utilize. When the webpage is accessed, the browser downloads the applet from a server and runs it on the user's machine (the client). Applets differ from apps 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 app 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 threat that is encoded as a macro embedded in a document. Many apps, such as Microsoft Word and Excel, support powerful macro languages.

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

Mail client

An email client is an app that enables you to send and receive email.

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 threat information database. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a threat, and does not generate false alarms.

Online predators

Individuals who seek to attract minors or adolescents into conversations on purpose to involve them into illegal sexual activities. Social networks are the ideal place where vulnerable children can easily be hunted and seduced into committing sexual activities, online or face-to-face.

Packed programs

A file in a compression format. Many operating systems and apps 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 email 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 email directs the user to visit a website 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 website, however, is bogus and set up only to steal the user's information.

Photon

Photon is an innovative non-intrusive Bitdefender technology, designed to minimize the performance impact of your security solution. By monitoring your PC's activity in the background, it creates usage patterns that help optimize booting and scanning processes.

Polymorphic virus

A threat that changes its form with each file it infects. Since they have no consistent binary pattern, such threats 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.

Ransomware

Ransomware is a malicious program that tries to make money from users by locking their vulnerable systems. CryptoLocker, CryptoWall,



and TeslaWall, are only some variants that hunt personal systems of users.

The infection can be spread by accessing spam emails, downloading email attachments, or installing apps, without letting the user know about what is happening on his system. Daily users and companies are targeted by ransomware hackers.

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 apps hide critical files using rootkits. However, they are mostly used to hide threats or to conceal the presence of an intruder into the system. When combined with threats, 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 email.

Spyware

Any software that covertly gathers user information through the user's internet connection without his or her knowledge, usually for advertising



purposes. Spyware apps 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 apps 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 email addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse threat 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 apps 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 apps can be startup items. Normally, an alias of a file is placed in this folder rather than the file itself.

Subscription

Purchase agreement that gives the user the right to use a particular product or service on a specific number of devices and for a certain period of time. An expired subscription can be automatically renewed using the information provided by the user at the first purchase.

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.

Threat

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

Threat Information Update

The binary pattern of a threat, used by the security solution to detect and eliminate the threat.

Trojan

A destructive program that masquerades as a benign app. Unlike malicious software programs and worms, Trojans do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse threats is a program that claims to rid your computer of threats but instead introduces threats 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 feature that allows you to manually check for updates, or let it automatically update the product.

Virtual Private Network (VPN)

Is a technology that enables a temporary and encrypted direct connection to a certain network over a less secure network. This way, sending and receiving data is secure and encrypted, difficult to be caught by snoopers. A proof of security is the authentication, which can be done only using a username and password.

Worm

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