trovaprezzi.it

Questo manuale d'istruzione è fornito da trovaprezzi.it. Scopri tutte le offerte per BitDefender Antivirus Plus 2019 o cerca il tuo prodotto tra le migliori offerte di Software

Bitdefender® ANTIVIRUS PLUS

USER'S GUIDE

Bitdefender Antivirus Plus
User's Guide

Publication date 07/12/2018

Copyright© 2018 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.

Bitdefender

Table of Contents

Installation 1

1. Preparing for installation 2

2. System requirements 3
   2.1. Minimum system requirements 3
   2.2. Recommended system requirements 3
   2.3. Software requirements 4

3. Installing your Bitdefender product 5
   3.1. Install from Bitdefender Central 5
   3.2. Install from installation disc 7

Getting started 12

4. The basics 13
   4.1. Opening the Bitdefender window 14
   4.2. Notifications 15
   4.3. Profiles 15
      4.3.1. Configure automatic activation of profiles 16
   4.4. Password-protecting Bitdefender settings 17
   4.5. Product reports 17
   4.6. Special offers notifications 18
   4.7. Antimalware Scan Interface 18

5. Bitdefender interface 19
   5.1. System tray icon 19
   5.2. Navigation menu 21
   5.3. Dashboard 21
      5.3.1. Security status area 22
      5.3.2. Autopilot 23
      5.3.3. Quick actions 23
   5.4. The Bitdefender sections 24
      5.4.1. **Protection** 24
      5.4.2. **Privacy** 26
   5.5. Security Widget 27
      5.5.1. Scanning files and folders 28
      5.5.2. Hide / show Security Widget 28

6. Bitdefender Central 30
   6.1. Accessing Bitdefender Central 30
   6.2. My Subscriptions 31
      6.2.1. Check available subscriptions 31
      6.2.2. Add a new device 31
      6.2.3. Renew subscription 32
      6.2.4. Activate subscription 32
   6.3. My Devices 33
   6.4. My Account 35

6.5. Notifications 35

7. Keeping Bitdefender up-to-date 36
7.1. Checking if Bitdefender is up-to-date 36
7.2. Performing an update 36
7.3. Turning on or off automatic update 37
7.4. Adjusting update settings 38
7.5. Continuous updates 38

How to 40

8. Installation 41
8.1. How do I install Bitdefender on a second computer? 41
8.2. How can I reinstall Bitdefender? 41
8.3. Where can I download my Bitdefender product from? 42
8.4. How can I change the language of my Bitdefender product? 43
8.5. How do I use my Bitdefender subscription after a Windows upgrade? 45
8.6. How can I upgrade to the latest Bitdefender version? 47

9. Subscriptions 49
9.1. How do I activate Bitdefender subscription using a license key? 49

10. Bitdefender Central 51
10.1. How do I log in to Bitdefender Central using another online account? 51
10.2. How do I turn off Bitdefender Central help messages? 51
10.3. I forgot the password I set for my Bitdefender account. How do I reset it? 52
10.4. How can I manage the logon sessions associated to my Bitdefender account? 53

11. Scanning with Bitdefender 54
11.1. How do I scan a file or a folder? 54
11.2. How do I scan my system? 54
11.3. How do I schedule a scan? 54
11.4. How do I create a custom scan task? 55
11.5. How do I except a folder from being scanned? 56
11.6. What to do when Bitdefender detected a clean file as infected? 56
11.7. How do I check what threats Bitdefender detected? 57

12. Privacy protection 59
12.1. How do I make sure my online transaction is secure? 59
12.2. How do I remove a file permanently with Bitdefender? 59
12.3. How can I manually restore encrypted files when the restoration process fails? 60

13. Useful Information 61
13.1. How do I test my security solution? 61
13.2. How do I remove Bitdefender? 61
13.3. How do I remove Bitdefender VPN? 62
13.4. How do I automatically shut down the computer after the scan is over? 63
13.5. How do I configure Bitdefender to use a proxy internet connection? 64
13.6. Am I using a 32 bit or a 64 bit version of Windows? 65
13.7. How do I display hidden objects in Windows? 65

13.8. How do I remove other security solutions? ... 66
13.9. How do I restart in Safe Mode? ... 67

Managing your security ... 69

14. Antivirus protection ... 70
14.1. On-access scanning (real-time protection) ... 71
14.1.1. Turning on or off real-time protection ... 71
14.1.2. Configuring the real-time protection advanced settings ... 71
14.1.3. Restoring the default settings ... 75
14.2. On-demand scanning ... 75
14.2.1. Scanning a file or folder for threats ... 75
14.2.2. Running a Quick Scan ... 76
14.2.3. Running a System Scan ... 76
14.2.4. Configuring a custom scan ... 77
14.2.5. Antivirus Scan Wizard ... 80
14.2.6. Checking scan logs ... 83
14.3. Automatic scan of removable media ... 83
14.3.1. How does it work? ... 83
14.3.2. Managing removable media scan ... 84
14.4. Scan hosts file ... 85
14.5. Configuring scan exceptions ... 85
14.5.1. Excepting files and folders from scanning ... 86
14.5.2. Excepting file extensions from scanning ... 86
14.5.3. Managing scan exceptions ... 87
14.6. Managing quarantined files ... 88

15. Advanced Threat Defense ... 89
15.1. Turning on or off Advanced Threat Defense ... 89
15.2. Checking detected malicious attacks ... 89
15.3. Adding processes to exceptions ... 90

16. Online Threat Prevention ... 91
16.1. Bitdefender alerts in the browser ... 92

17. Vulnerability ... 94
17.1. Scanning your system for vulnerabilities ... 94
17.2. Using automatic vulnerability monitoring ... 95
17.3. Wi-Fi Security Advisor ... 97
17.3.1. Turning on or off Wi-Fi Security Advisor notifications ... 98
17.3.2. Configuring Home Wi-Fi network ... 98
17.3.3. Public Wi-Fi ... 98
17.3.4. Checking information about Wi-Fi networks ... 99

18. Safe Files ... 101
18.1. Turning on or off Safe Files ... 101
18.2. Protect personal files from ransomware attacks ... 102
18.3. Configuring apps access ... 102
18.4. Protection at boot ... 103

19. Ransomware Remediation ... 104

19.1. Turning on or off Ransomware Remediation 104
19.2. Turning on or off automatic restore 104
19.3. Viewing files that were automatically restored 104
19.4. Restoring encrypted files manually 105
19.5. Adding applications to exceptions 105

20. Password Manager protection for your credentials 107
20.1. Create a new Wallet database 108
20.2. Import an existing database 108
20.3. Export the Wallet database 109
20.4. Synchronize your wallets in the cloud 109
20.5. Manage your Wallet credentials 109
20.6. Turning on or off the Password Manager protection 110
20.7. Managing the Password Manager settings 110

21. VPN 114
21.1. Installing VPN 114
21.2. Opening VPN 115
21.3. VPN interface 115
21.4. Subscriptions 116

22. Safepay security for online transactions 117
22.1. Using Bitdefender Safepay™ 118
22.2. Configuring settings 119
22.3. Managing bookmarks 120
22.4. Turning off Safepay notifications 121
22.5. Using VPN with Safepay 121

23. Data Protection 122
23.1. Deleting files permanently 122

24. USB Immunizer 123

System optimization 124

25. Profiles 125
25.1. Work Profile 126
25.2. Movie Profile 127
25.3. Game Profile 128
25.4. Public Wi-Fi Profile 129
25.5. Battery Mode Profile 130
25.6. Real-time optimization 131

Troubleshooting 132

26. Solving common issues 133
26.1. My system appears to be slow 133
26.2. Scan doesn't start 134
26.3. I can no longer use an app 137
26.4. What to do when Bitdefender blocks a safe website or online app 137
26.5. What to do if Bitdefender detects a safe app as ransomware 138

26.6. How to update Bitdefender on a slow internet connection 138
26.7. Bitdefender services are not responding 139
26.8. The Autofill feature in my Wallet doesn't work 140
26.9. Bitdefender removal failed 141
26.10. My system doesn't boot up after installing Bitdefender 142
27. Removing threats from your system 145
27.1. Bitdefender Rescue Mode (Rescue Environment in Windows 10) 145
27.2. What to do when Bitdefender finds threats on your computer? 149
27.3. How do I clean a threat in an archive? 150
27.4. How do I clean a threat in an email archive? 151
27.5. What to do if I suspect a file as being dangerous? 152
27.6. What are the password-protected files in the scan log? 152
27.7. What are the skipped items in the scan log? 153
27.8. What are the over-compressed files in the scan log? 153
27.9. Why did Bitdefender automatically delete an infected file? 153
Contact us 154
28. Asking for help 155
29. Online resources 157
29.1. Bitdefender Support Center 157
29.2. Bitdefender Support Forum 157
29.3. HOTforSecurity Portal 158
30. Contact information 159
30.1. Web addresses 159
30.2. Local distributors 159
30.3. Bitdefender offices 159
Glossary 162

INSTALLATION

1. PREPARING FOR INSTALLATION

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

- Make sure that the computer where you plan to install Bitdefender meets the minimum system requirements. If the computer does not meet all the minimum system requirements, Bitdefender will not be installed or, if installed, it will not work properly and it will cause system slowdowns and instability. For a complete list of system requirements, refer to "*System requirements*" (p. 3).
- Log on to the computer using an Administrator account.
- Remove any other similar software from the computer. 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.
- It is recommended that your computer be connected to the internet during the installation, even when installing from a CD/DVD. If newer versions of the app files included in the installation package are available, Bitdefender can download and install them.

2. SYSTEM REQUIREMENTS

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

- Windows 7 with Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10

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

Note

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

- 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. Minimum system requirements

- 2 GB available free hard disk space
- Dual Core 1.6 GHz processor
- 1 GB of memory (RAM)

2.2. Recommended system requirements

- 2,5 GB available free hard disk space (at least 800 MB on the system drive)
- Intel CORE Duo (2 GHz) or equivalent processor
- 2 GB of memory (RAM)

2.3. Software requirements

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

- Microsoft Edge 40 and higher
- Internet Explorer 10 and higher
- Mozilla Firefox 51 and higher
- Google Chrome 34 and higher

3. INSTALLING YOUR BITDEFENDER PRODUCT

You can install Bitdefender from the installation disc, or using the web installer downloaded on your computer from Bitdefender Central.

If your purchase covers more than one computer (for example, you purchased Bitdefender Antivirus Plus for 3 PCs), repeat the installation process and activate your product with the same account on every computer. The account you need to use is the one which contains your Bitdefender active subscription.

3.1. Install from Bitdefender Central

From Bitdefender Central you can download the installation kit corresponding to the purchased subscription. Once the installation process is complete, Bitdefender Antivirus Plus is activated.

To download Bitdefender Antivirus Plus from Bitdefender Central:

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

   - **Protect this device**

     Select this option and save the installation file.

   - **Protect other devices**

     Select this option, and then 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, then run the installer.

Validating the installation

Bitdefender first checks your system to validate the installation.

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

If an incompatible 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 computer to complete the removal of detected security solutions.

The Bitdefender Antivirus Plus 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 Plus.

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 Plus.

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.

Critical areas on your system are scanned for threats, the latest versions of the app files are downloaded and installed, and the Bitdefender services are started. This step can take a couple of minutes. Click **SKIP SCAN** if you want to scan your system later on. For more information about running a system scan, refer to "*Running a System Scan*" (p. 76).

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. Click **START USING Bitdefender** to continue.

Step 4 - Get started

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

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

3.2. Install from installation disc

To install Bitdefender from the installation disc, insert the disc in the optical drive.

A installation screen should be displayed in a few moments. Follow the instructions to start installation.

If the installation screen does not appear, use Windows Explorer to browse to the disc's root directory and double-click the file autorun.exe.

If your internet speed is slow, or your system is not connected to the internet, click the **Install from CD/DVD** button. In this case, the Bitdefender product available on the disc will be installed and a newer version will be downloaded from the Bitdefender servers via product update.

Validating the installation

Bitdefender first checks your system to validate the installation.

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

If an incompatible 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 computer to complete the removal of detected security solutions.

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 Plus.

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 Plus.

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.

Critical areas on your system are scanned for threats and the Bitdefender services are started. This step can take a couple of minutes. Click **SKIP SCAN** if you want to scan your system later on. For more information about running a system scan, refer to "*Running a System Scan*" (p. 76).

Step 3 - Installation completed

A summary of the installation is displayed. If any active threat was detected and removed during the installation, a system reboot may be required. Click **START USING Bitdefender** to continue.

Step 4 - 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. 30).

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 and include a digit.
  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 log 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**, and then type the email address and the password of your Bitdefender account.

   Click **SIGN IN** to continue.

2. If you forgot the password for your account or you simply want to reset the one you already set, click **Forgot my password**. Type your email address, then click **FORGOT PASSWORD**. Check your email account and follow the provided instructions to set a new password for your Bitdefender account.

   Note
   If you already have a MyBitdefender account, you can use it to log 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 log into your Bitdefender account.

- **I want to log in using my Microsoft, Facebook or Google account**

  To log 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 log in, or the personal information of your friends and contacts.

Step 5 - Activate your product

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

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

Proceed according to your situation:

- I have an activation code

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

  1. Type the activation code in the **I have an activation code** field, and then click **CONTINUE**.

     Note
     You can find your activation code:
     - on the CD/DVD label.
     - on the product registration card.
     - in the online purchase email.

  2. **I want to evaluate Bitdefender**

     In this case, you can use the product for a 30 day period. To begin the trial period, select **I don't have a subscription, I want to try the product for free**, and then click **CONTINUE**.

Step 6 - Get started

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

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

GETTING STARTED

4. THE BASICS

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

The app uses the Photon technology to enhance the speed and performance of the threat scanning process. It works by learning the usage patterns of your system apps to know what and when to scan, thus minimizing the impact on system performance.

Connecting to public wireless networks belonging to airports, malls, cafés, or hotels without protection may be dangerous for your device and data. Mainly because fraudsters may be watching your activity and find the best moment to steal personal data, but also because everyone can see your IP address; thus making your machine a victim for future cyberattacks. To avoid such unfortunate situations, install and use the "*VPN*" (p. 114) app.

You can keep track of your passwords and online accounts by storing them with "*Password Manager protection for your credentials*" (p. 107) in a wallet. With a single master password you are able to protect your privacy from intruders that may try to let you out of money.

To safeguard you from potential snoops and spies when your device is connected to an unsecured wireless network, Bitdefender analyzes its security level, and when necessary, comes with recommendations to boost the safety of your online activities. For instructions on how to keep your personal data secure, refer to "*Wi-Fi Security Advisor*" (p. 97).

Your personal files stored locally such as documents, photos or movies and also those stored in the cloud can stay now far away from the today's most dangerous threats, namely ransomware. For information on how to settle personal files to a shelter, refer to "*Safe Files*" (p. 101).

Files encrypted by ransomware can now be recovered without having to spend money for any requested ransom. For information on how to recover encrypted files, refer to "*Ransomware Remediation*" (p. 104).

While you work, play games or watch movies, Bitdefender can offer you a continuous user experience by postponing maintenance tasks, eliminating interruptions and adjusting system visual effects. You can benefit from all these by activating and configuring "*Profiles*" (p. 125).

Bitdefender will make most security-related decisions for you and will rarely show pop-up alerts. Details about actions taken and information about program operation are available in the Notifications window. For more information, refer to "*Notifications*" (p. 15).

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

To use the online features of Bitdefender Antivirus Plus and manage your subscriptions and devices, access your Bitdefender account. For more information, refer to "*Bitdefender Central*" (p. 30).

The "How to" (p. 40) section is where you will find step-by-step instructions on how to perform common tasks. If you experience issues while using Bitdefender, check the "*Solving common issues*" (p. 133) section for possible solutions to the most common problems.

4.1. Opening the Bitdefender window

To access the main interface of Bitdefender Antivirus Plus, follow the steps below:

- In **Windows 7**:
  1. Click **Start** and go to **All Programs**.
  2. Click **Bitdefender**.
  3. Click **Bitdefender Antivirus Plus** or, quicker, double-click the Bitdefender icon in the system tray.
- In **Windows 8 and Windows 8.1**:

  Locate Bitdefender from the Windows Start screen (for example, you can start typing "Bitdefender" directly in the Start screen), and then click its icon. Alternatively, open the Desktop app, and then double-click the Bitdefender icon in the system tray.
- In **Windows 10**:

  Type "Bitdefender" in the search box from the taskbar, and then click its icon. Alternatively, double-click the Bitdefender icon in the system tray.

For more information about the Bitdefender window and icon in the system tray, refer to "*Bitdefender interface*" (p. 19).

4.2. Notifications

Bitdefender keeps a detailed log of events concerning its activity on your computer. Whenever something relevant to the security of your system or data happens, a new message is added to the Bitdefender Notifications area, in a similar way to a new email appearing in your Inbox.

Notifications are an important tool in monitoring and managing your Bitdefender protection. For instance, you can easily check if the update was successfully performed, if threats or vulnerabilities were found on your computer, etc. Additionally, you can take further action if needed or change actions taken by Bitdefender.

To access the Notifications log, click **Notifications** on the navigation menu on the Bitdefender interface. Every time a critical event occurs, a counter can be noticed on the icon.

Depending on type and severity, notifications are grouped in:

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

Click each tab to find more details about the generated events. Brief details are displayed at a single-click on each event title, namely: a short description, the action Bitdefender took on it when it happened, and the date and time when it occurred. Options may be provided to take further action if needed.

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

4.3. Profiles

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

Bitdefender Profiles assigns more system resources to the running apps by temporarily modifying protection settings and adjusting system configuration. Consequently, the system impact on your activity is minimized.

To adapt to different activities, Bitdefender comes with the following profiles:

Work Profile
: Optimizes your work efficiency by identifying and adjusting the product and system settings.

Movie Profile
: Enhances visual effects and eliminates interruptions when watching movies.

Game Profile
: Enhances visual effects and eliminates interruptions when playing games.

Public Wi-Fi Profile
: Applies product settings to benefit from full protection while connected to an unsecure wireless network.

Battery Mode Profile
: Applies product settings and holds down background activity to save battery life.

4.3.1. Configure automatic activation of profiles

For an easy-to-use experience, you can configure Bitdefender to manage your working profile. In this case, Bitdefender automatically detects the activity you perform and applies system and product optimization settings.

To allow Bitdefender to activate profiles:

1. Click **Settings** on the navigation menu on the Bitdefender interface.
2. Select the **Profiles** tab.
3. Use the corresponding switch to turn on **Activate profiles automatically**.

If you do not wish for the Profiles to be automatically activated, turn off the switch.

To manually activate a profile, turn on the corresponding switch. Only one profile can be manually activated at once.

For more information on Profiles, refer to "*Profiles*" (p. 125)

4.4. Password-protecting Bitdefender settings

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

To configure password protection for the Bitdefender settings:

1. Click **Settings** on the navigation menu on the Bitdefender interface.
2. In the **General** window, turn on **Password protection**.
3. Type the password in the two fields, and then click **OK**. The password must be at least 8 characters long.

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

Important

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

To remove password protection:

1. Click **Settings** on the navigation menu on the Bitdefender interface.
2. In the **General** window, turn off **Password protection**.
3. Type the password, and then click **OK**.

Note

To modify the password for your product, click **Password change**. Type your current password, and then click **OK**. In the new window which appears type the new password you want to use from now on to restrict the access to your Bitdefender settings.

4.5. Product reports

Product reports contain information about how you use the Bitdefender product you have installed. This information is essential for improving the product and can help us offer you a better experience in the future.

Note that these reports contain no confidential data, such as your name or IP address, and that they are not be used for commercial purposes.

If during the installation process you have chosen to send such reports to the Bitdefender servers and now would like to stop the process:

1. Click **Settings** on the navigation menu on the Bitdefender interface.
2. Select the **Advanced** tab.
3. Turn off **Product reports**.

4.6. Special offers notifications

When promotional offers are available, the Bitdefender product is set up to notify you through a pop-up window. This gives you the opportunity to benefit from advantageous prices and keep your devices protected for a longer period of time.

To turn on or off special offers notifications:

1. Click **Settings** on the navigation menu on the Bitdefender interface.
2. In the **General** window, turn on or off the corresponding switch.

The special offers and product notifications option is enabled by default.

4.7. Antimalware Scan Interface

Bitdefender integrates with Microsoft Antimalware Scan Interface (AMSI), a way to help you stay protected from dynamic script-based malware and non-traditional avenues of cyberattack. AMSI is a generic interface standard that allows applications and services to integrate with Bitdefender products.

To turn on or off the integration with Antimalware Scan Interface:

1. Click **Settings** on the navigation menu on the Bitdefender interface.
2. In the **General** window, turn on or off the corresponding switch.

The integration with Antimalware Scan Interface option is enabled by default and is only available in Windows 10.

5. BITDEFENDER INTERFACE

Bitdefender Antivirus Plus 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 your Bitdefender account, the settings area, notifications and the Bitdefender sections for detailed configuration and advanced administrative tasks. 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.

5.1. System tray icon

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

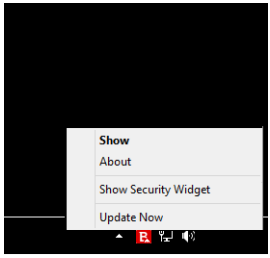
Note
The Bitdefender icon may not be visible at all times. To make the icon appear permanently:

- 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 **Properties**.
  2. Click **Customize** in the Taskbar window.
  3. Click the **Select which icons appear on the taskbar** link in the **Notifications & actions** window.
  4. 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.



Tray Icon

- **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 computer or how the product operates, by displaying a special symbol, as follows:

No issues are affecting the security of your system.
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: . 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.

5.2. Navigation menu

On the left side on 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, access Firewall settings, protect files and apps from ransomware attacks, recover data in case it gets encrypted by a ransowmware, and configure protection while surfing on the internet.
- **Privacy**. From here, you can create password managers for your online accounts, protect the access to your webcam from unwanted eyes, make online payments in a safe environment, and open the VPN app.
- **Notifications**. From here, you have access to the generated notifications.
- **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.
- **Settings**. From here, you have access to general settings.
- **Support**. From here, whenever you need assistance in solving a situation with your Bitdefender Antivirus Plus, you can contact the Bitdefender Technical Support department.

5.3. 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 computer'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.

5.3.1. Security status area

Bitdefender uses an issue tracking system to detect and inform you about the issues that may affect the security of your computer 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 computer, 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.

5.3.2. 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**.

5.3.3. 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 computer.
- **System Scan**. Run a system scan to make sure your computer is clean of threats.
- **Vulnerability Scan**. Scan your computer for vulnerabilities to make sure that all installed apps, along with the Operating System, are updated and properly functioning.
- **Check Wi-Fi safety**. Open Wi-Fi Security Advisor to check if the wireless home network you are connected to is secure or not and if it has vulnerabilities.
- **Wallets**. View and manage your wallets.
- **Open Safepay**. Open Bitdefender Safepay™ to protect your sensitive data while performing online transactions.
- **Open VPN**. Open Bitdefender VPN to add an extra layer of protection while connected to the internet.
- **File Shredder**. Launch the File Shredder tool to remove traces of sensitive data from your computer.
-

To start protecting additional devices with Bitdefender:

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

   You are redirected to the Bitdefender account webpage. Make sure that you are logged in with your credentials.

2. Click **SEND DOWNLOAD LINK** in the window that appears.

3. 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 Bitdefender check the email account that you typed in, and then press the corresponding download button.

Depending on your choice, the following Bitdefender products will be installed:

- Bitdefender Antivirus Plus on Windows-based devices.
- Bitdefender Antivirus for Mac on macOS-based devices.
- Bitdefender Mobile Security on Android-based devices.
- Bitdefender Mobile Security on iOS-based devices.

5.4. The Bitdefender sections

The Bitdefender product comes with two sections divided into useful features to help you stay protected while you work, surf the web, play games, or want make online payments.

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

5.4.1. **Protection**

In the Protection section you can configure your advanced security settings, set up the Safe Files and Online Threat Prevention features, check and fix potential system vulnerabilities and assess the security of the wireless networks you connect to.

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
- Rescue Mode (Rescue Environment in Windows 10)

For more information about scan tasks and how to configure antivirus protection, refer to "*Antivirus protection*" (p. 70).

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. 91).

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. 89).

VULNERABILTY

The Vulnerability feature helps you keep the operating system and the apps you regularly use up to date and to identify the insecure wireless networks you connect to.

Click **Vulnerability Scan** in the Vulnerability feature to start identifying critical Windows updates, apps updates, weak passwords belonging to Windows accounts and wireless networks that are not secure.

Click **Wi-Fi security** to view the list of the wireless networks you connect to, along with our reputation assessment for each of them and the actions you can take to stay safe from potential snoops.

For more information on configuring vulnerability protection, refer to "*Vulnerability*" (p. 94).

SAFE FILES

The Safe Files feature ensures that your personal files stay protected from ransomware attacks.

For more information about how to configure Safe Files to protect your personal files from ransomware attacks, refer to "*Safe Files*" (p. 101).

RANSOMWARE REMEDIATION

The Ransomware Remediation feature helps you recover files in case they get encrypted by ransomware.

For more information about how to recover encrypted files, refer to "*Ransomware Remediation*" (p. 104).

5.4.2. Privacy

In the Privacy section you can open the Bitdefender VPN app, protect your online transactions and keep your browsing experience secure.

The features you can manage in the Privacy section are:

VPN

VPN secures your online activity and hides your IP address each time you connect to unsecured wireless networks while in airports, malls, cafés, or hotels. Additional, you can access content that normally is restricted in certain areas.

For more information about this feature, refer to "*VPN*" (p. 114).

PASSWORD MANAGER

Bitdefender Password Manager helps you keep track of your passwords, protects your privacy and provides a secure browsing experience.

For more information about configuring Password Manager, refer to "*Password Manager protection for your credentials*" (p. 107).

SAFEPAY

The Bitdefender Safepay™ browser helps you to keep your online banking, e-shopping and any other type of online transaction private and secure.

For more information about Bitdefender Safepay™, refer to "*Safepay security for online transactions*" (p. 117).

DATA PROTECTION

The Data Protection feature lets you delete files permanently.
Click **File Shredder** in the Data Protection pane to start a wizard that will allow you to completely eliminate files from your system.

For more information on configuring Data Protection, refer to "*Data Protection*" (p. 122).

5.5. Security Widget

Security Widget is the quick and easy way to monitor and control Bitdefender Antivirus Plus. 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.

Security 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.

Critical issues are affecting the security of your system.

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

Non-critical issues are affecting the security of your system. You should check and fix them when you have the time. Click the status icon to begin fixing the reported issues.

Your system is protected.

When an on-demand scan task is in progress, this animated 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 for one unread event, to open the Notifications window. For more information, refer to "*Notifications*" (p. 15).

5.5.1. 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.

5.5.2. 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 icon.
  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.

6. 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 log in to your Bitdefender account from any computer 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 logged in, you can start doing the following:

- Download and install Bitdefender on Windows, macOS, iOS and Android operating systems. The products available for download are:
  - Bitdefender Antivirus Plus
  - Bitdefender Antivirus for Mac
  - Bitdefender Mobile Security for Android
  - Bitdefender Mobile Security for iOS
- Manage and renew your Bitdefender subscriptions.
- Add new devices to your network and manage them wherever you are.

6.1. Accessing Bitdefender Central

There are several ways to access Bitdefender Central:

- From the Bitdefender main interface:
  1. Click **My Account** on the navigation menu on the Bitdefender interface.
  2. Click **Go to Bitdefender Central**.
  3. Log 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. Log in to your Bitdefender account using your email address and password.

- From your Android or iOS 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.

6.2. My Subscriptions

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

6.2.1. 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.

You can add a new device to a subscription or renew it by selecting a subscription card.

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

6.2.2. Add a new device

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

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

- **Protect this device**

  Select this option and save the installation file.

- **Protect other devices**

  Select this option, and then 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, then run the installer.

6.2.3. Renew subscription

If you did not opt out for automatically renewing your Bitdefender subscription, you can manually renew it by following these steps:

1. Access Bitdefender Central.
2. Select the **My Subscriptions** panel.
3. Select the desired subscription card.
4. Click **RENEW** to continue.

A webpage opens in your web browser where you can renew your Bitdefender subscription.

6.2.4. Activate subscription

A 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 **ACTIVATION 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 select **INSTALL PROTECTION** to install the product on one of your devices.

6.3. 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, 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 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 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 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 the desired device card.

Once you click 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, the status of Bitdefender VPN 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 "*Running a System Scan*" (p. 76) and to "*Running a Quick Scan*" (p. 76).
- **Vulnerability**. To check a device for any vulnerabilities such as missing Windows updates, outdated apps, or weak passwords click the **SCAN** button in the Vulnerability tab. Vulnerabilities cannot be fixed remotely. In case any vulnerability is found, you need to run a new scan on the device and then take the recommended actions. Click **More details** to access a detailed report about the found issues. For more details about this feature, refer to "*Vulnerability*" (p. 94).

6.4. My Account

In the **My Account** area you have the possibility to personalize your profile, change the password associated to your account, manage the logon sessions and the Bitdefender Central help messages.

Once you click the icon in the upper right side of the screen and choose **My Account**, you have the following tabs:

- **Profile** - here you can add and edit account information.
- **Change password** - from here you can change the password associated to your account.
- **Session management** - here you can view and manage the latest inactive and active logon sessions running on devices associated to your account.
- **Settings** - here you can turn on and off the Bitdefender Central help messages and decide whether to be notified or not when snap photos are taken on your Android devices.

6.5. 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.

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

The update process is performed on the fly, meaning that the files to be updated are replaced progressively. 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 computer connects to the internet through a proxy server, you must configure the proxy settings as described in "*How do I configure Bitdefender to use a proxy internet connection?*" (p. 64).
- 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. 36).

7.1. 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.

7.2. 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 computer 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 the desired device card, and then the icon in the upper-right corner of the screen.
4. Select **Update**.

7.3. 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, permanently 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.

7.4. 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 computer. This is to prevent the Bitdefender update process from interfering with the user's work.

If you want to be prompted when an update requires a restart, turn on **Restart notification**.

7.5. 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.

Note

The updates including new features and improvements will be delivered only to users who have Bitdefender 2018 installed.

HOW TO

8. INSTALLATION

8.1. How do I install Bitdefender on a second computer?

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

To install Bitdefender on a second computer:

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

   You are redirected to the Bitdefender account webpage. Make sure that you are logged in with your credentials.

2. Click **SEND DOWNLOAD LINK** in the window that appears.

3. 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 Bitdefender check the email account that you typed in, and then press the corresponding download button.

4. Run the Bitdefender product you have downloaded.

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

8.2. 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 Plus** and select **Uninstall**.
3. Click **REINSTALL** in the window that appears.
4. You need to restart the computer 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 Plus** and select **Uninstall**.
  4. Click **REINSTALL** in the window that appears.
  5. You need to restart the computer 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 Plus** and select **Uninstall**.
  4. Click **Uninstall** again to confirm your choice.
  5. Click **REINSTALL**.
  6. You need to restart the computer 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.

8.3. Where can I download my Bitdefender product from?

You can install Bitdefender from the installation disc, or using the web installer you can download on your computer from the Bitdefender Central platform.

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 computer, the system becomes unstable.

To install Bitdefender from Bitdefender Central:

1. Access Bitdefender Central.
2. Select the **My Devices** panel, and then click **INSTALL PROTECTION**.
3. Choose one of the two available options:
   - **Protect this device**

     Select this option and save the installation file.
   - **Protect other devices**

     Select this option, and then 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. Run the Bitdefender product you have downloaded.

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

If you want to use Bitdefender in another language, you will have to reinstall the product with the proper language.

To use Bitdefender in another language:

1. Remove Bitdefender by following these steps:
   - In **Windows 7**:
     a. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
     b. Find **Bitdefender Antivirus Plus** and select **Uninstall**.

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

d. 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 **Bitdefender Antivirus Plus** and select **Uninstall**.

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

e. 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 **Bitdefender Antivirus Plus** 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.

2. Change the language of Bitdefender Central:

a. Access Bitdefender Central.

b. Click the icon in the upper right side of the screen.

c. Click **My Account** in the slide menu.

d. Select the **Profile** tab.

e. Select a language from the **Language** drop-down list box, and then click **SAVE**.

3. Download the installation file:

a. Select the **My Devices** panel, and then click **INSTALL PROTECTION**.

b. Choose one of the two available options:

- **Protect this device**

  Select this option and save the installation file.

- **Protect other devices**

  Select this option, and then 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 Bitdefender check the email account that you typed in, and then click the corresponding download button.

4. Run the Bitdefender product you have downloaded.

Note
This reinstall procedure will permanently delete the customized settings.

8.5. How do I use my Bitdefender subscription after a Windows upgrade?

This situation appears when you upgrade your operating system and you want to continue using your Bitdefender subscription.

If you are using a previous Bitdefender version you can upgrade, free of charge, to the latest Bitdefender, as follows:

- From a previous Bitdefender Antivirus version to the latest Bitdefender Antivirus available.
- From a previous Bitdefender Internet Security version to the latest Bitdefender Internet Security available.
- From a previous Bitdefender Total Security version to the latest Bitdefender Total Security available.

There are two cases which may appear:

- You have upgraded the operating system using Windows Update and you notice Bitdefender is no longer working.

  In this case, you need to reinstall the product by following these steps:

  - In **Windows 7**:

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

   Open the interface of your new installed Bitdefender product to have access to its features.

- 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 Plus** and select **Uninstall**.
4. Click **REINSTALL** in the window that appears.
5. Wait for the uninstall process to complete, and then reboot your system.

   Open the interface of your new installed Bitdefender product to have access to its features.

- 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 Plus** and select **Uninstall**.
4. Click **Uninstall** again to confirm your choice.
5. Click **REINSTALL** in the window that appears.
6. Wait for the uninstall process to complete, and then reboot your system.

   Open the interface of your new installed Bitdefender product to have access to its features.

> **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.

- You changed your system and you want to continue using the Bitdefender protection. Therefore, you need to reinstall the product using the latest version.

  To solve this situation:

  1. Download the installation file:
     a. Access Bitdefender Central.
     b. Select the **My Devices** panel, and then click **INSTALL PROTECTION**.
     c. Choose one of the two available options:
        - **Protect this device**

          Select this option and save the installation file.
        - **Protect other devices**

          Select this option, and then 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.
  2. Run the Bitdefender product you have downloaded.

  For more information about the Bitdefender installation process, refer to "*Installing your Bitdefender product*" (p. 5).

8.6. How can I upgrade to the latest Bitdefender version?

From now on, the upgrade to the newest version is possible without following the manual uninstall and reinstall procedure. More exactly, the new product including new features and major product improvements is delivered via

product update and, if you already have an active Bitdefender subscription, the product gets automatically activated.

If you are using the 2018 version, you can upgrade to the newest version by following these steps:

1. Click **RESTART NOW** in the notification you receive with the upgrade information. If you miss it, access the Notifications window, point to the most recent update, and then click the **RESTART NOW** button. Wait for the computer to restart.

   The **What's new** window with information about the improved and new features appears.

2. Click the **Read more** links to be redirected to our dedicated page with more details and helpful articles.

3. Close the **What's new** window to access the interface of the new installed version.

Users that want to upgrade for free from Bitdefender 2016 or a lower version to the newest Bitdefender version, have to remove their current version from Control Panel, and then download the latest installation file from the Bitdefender website at the following address: https://www.bitdefender.com/Downloads/. The activation is possible only with a valid subscription.

9. SUBSCRIPTIONS

9.1. How do I activate Bitdefender subscription using a license key?

If you have a valid license key and want to use it to activate a subscription for Bitdefender Antivirus Plus, there are two possible cases:

- You have upgraded from a previous Bitdefender version to the new one:
  1. Once the upgrade to Bitdefender Antivirus Plus is complete, you are asked to log in to your Bitdefender account.
  2. Click **Sign In**, and then type the email address and the password of your Bitdefender account.
  3. Click **SIGN IN** to continue.
  4. A notification informing you that a subscription was created appears on your account screen. The created subscription will be valid for the remaining days on your license key and for the same number of users.

     Devices that are using previous Bitdefender versions and are registered with the license key you have converted to a subscription need to activate the product with the same Bitdefender account.
- Bitdefender was not previously installed on the system:
  1. As soon as the installation process is complete, you are asked to log in to your Bitdefender account.
  2. Click **Sign In**, and then type the email address and the password of your Bitdefender account.
  3. Click **SIGN IN** to continue, and then the **FINISH** button to access the Bitdefender Antivirus Plus interface.
  4. Click **My Account** on the navigation menu on the Bitdefender interface.
  5. Click **Activate Now**.

     A new window appears.
  6. Click the **Get your FREE upgrade now!** link.

7. Type in your license key in the corresponding field and click **UPGRADE MY PRODUCT**. A subscription with the same availability and number of users of your license key is associated to your account.

10. BITDEFENDER CENTRAL

10.1. How do I log in to Bitdefender Central using another online account?

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

To successfully use another account:

1. Click **My Account** on the navigation menu on the Bitdefender interface.
2. Click **Switch Account** on the upper right corner of the screen to change the account linked to the computer.
3. Type the email address and the password of your account in the corresponding fields, 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. 155).

10.2. 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. Select the **Settings** tab.
5. Disable the **Turn on/off help messages** option.

10.3. 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 **My Account** on the navigation menu on the Bitdefender interface.
  2. Click **Switch Account** on the upper right corner of the screen.

     A new window appears.
  3. Click **Forgot my password**.
  4. Type the email address used to create your Bitdefender account, and then click **FORGOT PASSWORD**.
  5. Check your email and click the provided button.

     The Bitdefender RESET PASSWORD window opens.
  6. Type your email address and the new password in the corresponding field. The password must be at least 8 characters long and include numbers.
  7. Click **RESET PASSWORD**.
- From your web browser:
  1. Go to: https://central.bitdefender.com.
  2. Click **Forgot my password**.
  3. Type your email address, and then click **FORGOT PASSWORD**.
  4. 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.

10.4. 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 **My Account** in the slide menu.
4. Select the **Session management** tab.
5. In the **Active sessions** area, select the **SIGN OUT** option next to the device you want to finish the logon session.

11. SCANNING WITH BITDEFENDER

11.1. 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 computer.

11.2. 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 **System Scan**.
3. 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. 80).

11.3. 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 computer.

To schedule a scan:

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

2. In the **ANTIVIRUS** pane, click **Manage Scans**.
3. Choose the scan type that you want to schedule, Full System Scan or Quick Scan, then click **SCAN OPTIONS**.

   Alternatively, you can create a scan type to suit your needs by clicking **NEW CUSTOM TASK**.
4. Enable the **Schedule** option.

   Select one of the corresponding options to set a schedule:

   - At system startup
   - Once
   - Periodically

In the **Scan targets** window you can select the locations you want to be scanned. This option is only available if you choose to create a new custom scan.

11.4. How do I create a custom scan task?

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

To create a customized scan task, proceed as follows:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **ANTIVIRUS** pane, click **Manage Scans**.
3. Click **NEW CUSTOM TASK**. In the **Basic** window enter a name for the scan and select the locations to be scanned.
4. If you want to configure the scanning options in detail, select the **Advanced** tab.

   You can easily configure the scanning options by adjusting the scan level. Drag the slider along the scale to set the desired scan level.

   You can also choose to shutdown the computer when the scan is over if no threats are found. Remember that this will be the default behavior every time you run this task.
5. Click **OK** to save the changes and close the window.
6. Use the corresponding switch if you want to set a schedule for your scan task.

7. Click **START SCAN** and follow the scan wizard to complete the scan. At the end of the scan, you will be prompted to choose the actions to be taken on the detected files, if any.
8. If you want to, you can quickly rerun a previous custom scan by clicking the corresponding entry in the available list.

11.5. 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 **Settings**.
3. Click the **Exceptions** tab.
4. Click the **List of files and folders excepted from scanning** accordion menu, and then **Add**.
5. Click **BROWSE**, select the folder that you want to be excepted from scanning, and then choose the type of scanning it should be excepted from.
6. Click **ADD** to save the changes and close the window.

11.6. 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 **Settings**.
   c. In the **Shield** 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. 65).
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 **Quarantine**.
   c. 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. 56).
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. 155).

11.7. 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**.

12. PRIVACY PROTECTION

12.1. How do I make sure my online transaction is secure?

To make sure your online operations remain private, you can use the browser provided by Bitdefender to protect your transactions and home banking apps.

Bitdefender Safepay™ is a secured browser designed to protect your credit card information, account number or any other sensitive data you may enter while accessing different online locations.

To keep your online activity secure and private:

1. Click **Privacy** on the navigation menu on the Bitdefender interface.
2. In the **Safepay** pane, click **Open Safepay**.
3. Click the button to access the **Virtual Keyboard**.

   Use the **Virtual Keyboard** when typing sensitive information such as your passwords.

12.2. How do I remove a file permanently with Bitdefender?

If you want to remove a file permanently from your system, you need to delete the data physically from your hard disk.

The Bitdefender File Shredder will help you to quickly shred files or folders from your computer using the Windows contextual menu by following these steps:

1. Right-click the file or folder you want to permanently delete, point to Bitdefender and select **File Shredder**.
2. Click **DELETE PERMANENTLY**, and then confirm that you wish to continue with the process.

   Wait for Bitdefender to finish shredding the files.
3. The results are displayed. Click **FINISH** to exit the wizard.

12.3. How can I manually restore encrypted files when the restoration process fails?

In case encrypted files cannot be automatically restored, you can manually restore them by following these steps:

1. Click **Notifications** on the navigation menu on the Bitdefender interface.
2. In the **All** tab, select the notification regarding the latest ransomware behavior detected, and then click **Encrypted Files**.
3. The list with the encrypted files is displayed.

   Click **RECOVER FILES** to continue.
4. In case the entire or a part of the restoring process fails, you have to choose the location where the decrypted files should be saved. Click **RESTORE LOCATION**, and then choose a location on your PC.
5. A confirmation window appears.

   Click **FINISH** to end the restoring process.

Files with the following extensions can be restored in case they get encrypted:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

13. USEFUL INFORMATION

13.1. 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 **eicar.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. 155).

13.2. How do I remove Bitdefender?

If you want to remove your Bitdefender Antivirus Plus:

- In **Windows 7**:
  1. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
  2. Find **Bitdefender Antivirus Plus** 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 Plus** 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 Plus** 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.

13.3. How do I remove Bitdefender VPN?

The procedure of removing Bitdefender VPN is similar to the one you use to remove other programs from your computer:

- In **Windows 7**:
  1. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
  2. Find **Bitdefender VPN** and select **Uninstall**.

     Wait for the uninstall process to complete.
- 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 VPN** and select **Uninstall**.

Wait for the uninstall process to complete.

- 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 VPN** and select **Uninstall**.
  4. Click **Uninstall** again to confirm your choice.

     Wait for the uninstall process to complete.

13.4. How do I automatically shut down the computer 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 computer 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 at the computer and you want to go to sleep. You would like to have your entire system checked for threats by Bitdefender.

This is how you set up Bitdefender to shut down your system at the end of the scan:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **ANTIVIRUS** pane, click **Manage Scans**.
3. In the **Manage Scan Tasks** window, click **NEW CUSTOM TASK** to enter a name for the scan and select the locations to be scanned.
4. If you want to configure the scanning options in detail, select the **Advanced** tab.
5. Choose to shutdown the computer when the scan is over if no threats are found.
6. Click **OK** to save the changes and close the window.
7. Click **START SCAN** to scan your system.

If no threats are found, the computer 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. 80).

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

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

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

To manage the proxy settings:

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.

13.6. 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.

13.7. 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**.

13.8. How do I remove other security solutions?

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

When you use more than one security solution on the same computer, the system becomes unstable. The Bitdefender Antivirus Plus 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 **Installed 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.

13.9. 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 computer.

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

14. ANTIVIRUS PROTECTION

Bitdefender protects your computer 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 computer 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 computer to make sure it can be safely accessed. For more information, refer to "*Automatic scan of removable media*" (p. 83).

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. 85).

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. 88).

If your computer has been infected with threats, refer to "*Removing threats from your system*" (p. 145). To help you clean your computer of threats that cannot be removed from within the Windows operating system, Bitdefender provides you with"*Bitdefender Rescue Mode (Rescue Environment in Windows 10)*" (p. 145). This is a trusted environment, especially designed for threat removal, which enables you to boot your computer independent of Windows.

When the computer runs in Rescue Mode (Rescue Environment in Windows 10), Windows threats are inactive, making it easy to remove them.

14.1. 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.

14.1.1. 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 **Settings**.
3. In the **Shield** 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.

14.1.2. Configuring the real-time protection advanced settings

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

To configure the real-time protection advanced settings:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **ANTIVIRUS** pane, click **Settings**.
3. In the **Shield** window, click the **Show advanced settings** accordion menu.

A paned window is displayed.

4. Scroll down on the window to configure the scan settings as needed.

Information on the scan options

You may find this information useful:

- **Scan only applications.** You can set Bitdefender to scan only accessed apps.
- **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 network shares.** To safely access a remote network from your computer, we recommend you to keep the Scan network shares option enabled.
- **Scan inside archives.** Scanning inside archives is a slow and resource-intensive process, which is therefore not recommended for real-time protection. Archives containing infected files are not an immediate threat to the security of your system. The threat can affect your system only if the infected file is extracted from the archive and executed without having real-time protection enabled.

  If you decide on using this option, turn it on, and then drag the slider along the scale to set a maximum accepted size limit (in MB) of archives to be scanned on-access.
- **Scan emails.** To prevent threats from being downloaded to your computer, Bitdefender automatically scans incoming and outgoing emails.

  Though not recommended, you can disable email threat scan to increase system performance. If you disable the corresponding scan options, the emails and files received will not be scanned, thus allowing infected files to be saved to your computer. This is not a major threat because real-time protection will block the threat when the infected files are accessed (opened, moved, copied or executed).

- **Scan boot sectors.** You can set Bitdefender to scan the boot sectors of your hard disk. This sector of the hard disk contains the necessary computer code to start the boot process. When a 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 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 for 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.
- **Scan at system boot.** Select the **Early boot scan** option to scan your system at startup as soon as all its critical services are loaded. The mission of this feature is to improve threat detection at system startup and the boot time of your system.

Actions taken on detected threats

You can configure the actions taken by the real-time protection by following these steps:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **ANTIVIRUS** pane, click **Settings**.
3. In the **Shield** window, click the **Show advanced settings** accordion menu.

   A paned window is displayed.
4. Scroll down on the window until you see the **Threat actions** option.
5. Configure the scan settings as needed.

The following actions can be taken by the real-time protection in Bitdefender:

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. 88).

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, a threat 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.

Move to quarantine

Moves detected files to quarantine. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. For more information, refer to "*Managing quarantined files*" (p. 88).

Deny access

In case an infected file is detected, the access to this will be denied.

14.1.3. 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 **Settings**.
3. In the **Shield** window, click the **Show advanced settings** accordion menu.

   A paned window is displayed.
4. Scroll down on the window until your see the **Reset settings** option. Select this option to reset the antivirus settings to default.

14.2. On-demand scanning

The main objective for Bitdefender is to keep your computer clean of threats. This is done by keeping new threats out of your computer 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 computer for resident threats after you've installed Bitdefender. And it's definitely a good idea to frequently scan your computer 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 computer whenever you want by running the default tasks or your own scan tasks (user-defined tasks). If you want to scan specific locations on your computer or to configure the scan options, configure and run a custom scan.

14.2.1. 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.

14.2.2. 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 **Quick Scan**.
3. 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.

14.2.3. Running a System Scan

The System Scan task scans the entire computer 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 computer.

Before running a System Scan, the following are recommended:

- Make sure Bitdefender is up-to-date with its threat information database. Scanning your computer 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. 36).
- Shut down all open programs.

If you want to scan specific locations on your computer or to configure the scanning options, configure and run a custom scan. For more information, refer to "*Configuring a custom scan*" (p. 77).

To run a System Scan:

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

3. The first time you run a System Scan, you are introduced into the feature. Click **OK, GOT IT** to continue.
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.

14.2.4. Configuring a custom scan

To configure a custom scan in detail and then run it:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **ANTIVIRUS** pane, click **Manage Scans**.
3. Click **NEW CUSTOM TASK**. In the **Basic** window enter a name for the scan and select the locations to be scanned.
4. If you want to configure the scanning options in detail, select the **Advanced** tab. A new window appears. Follow these steps:
   a. You can easily configure the scanning options by adjusting the scan level. Drag the slider along the scale to set the desired scan level. Use the description on the right side of the scale to identify the scan level that better fits your needs.

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

   b. You can also configure these general options:

      - **Run the task with low priority.** Decreases the priority of the scan process. You will allow other programs to run faster and increase the time needed for the scan process to finish.
      - **Minimize Scan Wizard to system tray.** Minimizes the scan window to the system tray. Double-click the Bitdefender icon to open it.
      - Specify the action to be taken if no threats are found.

   c. Click **OK** to save the changes and close the window.
5. If you want to set a schedule for your scan task, use the **Schedule** switch in the **Basic** window. Select one of the corresponding options to set a schedule:

- At system startup
- Once
- Periodically

6. Click **START SCAN** and follow the Antivirus Scan wizard to complete the scan. Depending on the locations to be scanned, the scan may take a while. At the end of the scan, you will be prompted to choose the actions to be taken on the detected files, if any.
7. If you want to, you can quickly rerun a previous custom scan by clicking the corresponding entry in the available list.

Information on the scan options

You may find this information useful:

- If you are not familiar with some of the terms, check them in the glossary. You can also find useful information by searching the internet.
- **Scan files.** You can set Bitdefender to scan all types of files or apps (program files) only. Scanning all files provides best protection, while scanning apps only can be used to perform a quicker scan.

  Apps (or program files) are far more vulnerable to threat attacks than other types of files. This category includes the following file extensions: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
- **Scan options for archives.** Archives containing infected files are not an immediate threat to the security of your system. The 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.

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

- **Scan boot sectors.** You can set Bitdefender to scan the boot sectors of your hard disk. This sector of the hard disk contains the necessary computer code to start the boot process. When a 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 computer.
- **Scan only new and changed files.** By scanning only new and modified files, you may greatly improve overall system responsiveness with a minimum trade-off in security.
- **Ignore commercial keyloggers.** Select this option if you have installed and use commercial keylogger software on your computer. Commercial keyloggers are legitimate computer monitoring software whose most basic function is to record everything that is typed on the keyboard.
- **Scan for rootkits.** Select this option to scan for rootkits and objects hidden using such software.
- **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).

14.2.5. 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 object 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. 88).

  ### 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. The log is provided in .xml format and can be locally saved by clicking the **Save Log** button, and then choosing a location.

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. 145).

14.2.6. 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**.

14.3. Automatic scan of removable media

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

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.

14.3.1. 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. 145).

14.3.2. Managing removable media scan

To manage automatic scan of removable media:

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

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

3. Select the **Drives and devices** tab.

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.

14.4. Scan hosts file

The hosts file comes by default with your operating system installation and is used to map hostnames to IP addresses each time you access a new webpage, connect to a FTP or to other internet servers. It is a plain text file and malicious programs may modify it. Advanced users know how to use it to block annoying ads, banners, third-party cookies, or hijackers.

To configure scan hosts file:

1. Click **Settings** on the navigation menu on the Bitdefender interface.
2. Select the **Advanced** tab.
3. Turn on or off **Scan hosts file**.

14.5. 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 system and contextual scanning. System scanning is an on-demand scanner which gives you the possibility to analyze the entire system for malicious threats that may endanger the security of your data. 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**.

14.5.1. 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 **Settings**.
3. Select the **Exceptions** tab.
4. Click the **List of files and folders excepted from scanning** accordion menu. In the window that appears, you can manage the files and folders excepted from scanning.
5. Add exceptions by following these steps:
   a. Click **Add**.
   b. Click **BROWSE**, select the file or folder that you want to be excepted from scanning, and then click **ADD**. Alternatively, you can type (or copy and paste) the path to the file or folder in the edit field.
   c. By default, the selected file or folder is excepted from both on-access and on-demand scanning. To change when to apply the exception, select one of the other options.
   d. Click **Add**.

14.5.2. 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 computer. 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 computer 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 **Settings**.
3. Select the **Exceptions** tab.

4. Click the **List of extensions excepted from scanning** accordion menu. In the window that appears, you can manage the file extensions excepted from scanning.
5. Add exceptions by following these steps:
   a. Click **Add**.
   b. Type the extensions that you want to be excepted from scanning, separating them with semicolons (;). Here is an example:

      txt;avi;jpg

   c. By default, all files with the specified extensions are excepted from both on-access and on-demand scanning. To change when to apply the exception, select one of the other options.
   d. Click **ADD**.

14.5.3. 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 **Settings**.
3. Select the **Exceptions** tab.
4. Use the options in the **List of files and folders excepted from scanning** accordion menu to manage scan exceptions.
5. To remove or edit scan exceptions, click one of the available links. Proceed as follows:
   - To remove an entry from the list, select it and click **Remove**.
   - To edit an entry from the table, double-click it (or select it and click **Edit**). A new window appears where you can change the extension or the path to be excepted and the type of scanning you want them to be excepted from, as needed. Make the necessary changes, then click **MODIFY**.

14.6. 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 **Quarantine**.

   Here you can view the name of the quarantined files, their original location and the name of the detected threats.
3. 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.
4. 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**.

15. 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 computer, 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.

15.1. 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, turn on or off the switch.

> **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.

15.2. Checking detected malicious attacks

Whenever threats or potentially malicious processes are detected, Bitdefender will block them to prevent your computer 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 **Threat Defense**.
3. The first time you access Ransomware Protection, you are introduced into the feature. Click **OK, GOT IT** to continue.

   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.

15.3. 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 **Settings**.
3. In the **Exceptions** window, click **Add applications to exceptions**.
4. Find and select the app you want to be excepted, and then click **OK**.

   To remove an entry from the list, click the **Remove** option next to it.

16. 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** window, 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 recommended you to keep enabled the Encrypted web scan option.

- Protection against fraud.

- Phishing protection.

In the **Network threat prevention** window, you have the **Network threat prevention** option. To keep your computer away from attacks made by complex malware (such as ransomware) through the exploitation of vulnerabilities, keep this option enabled.

You can create a list of websites that will not be scanned by the Bitdefender anti-threat, antiphishing and antifraud engines. The list should contain only websites you fully trust. For example, add the websites where you shop online.

To configure and manage websites 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 **Exceptions**.
3. Type the name of the website you want to add to the whitelist in the corresponding field, and then click **ADD**.

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

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

16.1. 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 webpage by clicking **TAKE ME BACK TO SAFETY**.
- Proceed to the webpage, despite the warning, by clicking **I understand the risks, take me there anyway**.
- If you are sure that the detected webpage is safe, click **SUBMIT** to add it to the whitelist. We recommend you to add only webpages that you fully trust.

17. VULNERABILITY

An important step in protecting your computer against malicious actions and apps is to keep the operating system and the apps you regularly use up to date. Moreover, to prevent unauthorized physical access to your computer, strong passwords (passwords that cannot be easily guessed) must be configured for each Windows user account and for the Wi-Fi networks you connect to as well.

Bitdefender automatically checks your system for vulnerabilities and alerts you about them. It scans for the following:

- outdated apps on your computer.
- missing Windows updates.
- weak passwords to Windows user accounts.
- not secured wireless networks and routers.

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

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

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

17.1. Scanning your system for vulnerabilities

To fix system vulnerabilities using the Vulnerability Scan option:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **VULNERABILITY** pane, click **Vulnerability Scan**.
3. Wait for Bitdefender to check your system for vulnerabilities. To stop the scanning process, click the **Skip** button at the top of the window.
   - **Critical Windows updates**

     Click **View details** to see the list of critical Windows updates that are not installed on your computer.

     To initiate the installation of selected updates, click **Install updates**. Please note that it may take a while to install the updates and some of

them may require a system restart to complete the installation. If required, restart the system at your earliest convenience.

- **Application updates**

  If an app is not up to date, click the **Download new version** link to download the latest version.

  Click **View details** to see information about the app that needs to be updated.

- **Weak Windows account passwords**

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

  Click **Change password at login** to set a new password for your system.

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

- **Wi-Fi networks**

  Click **View details** to find out more about the wireless network you are connected to. If it is recommended to set a stronger password for your home network, click the corresponding link.

  When other recommendations are available, follow the provided instructions to make sure your home network stays safe from the hackers' prying eyes.

In the upper-right corner of the window you can filter the results according to your preferences.

17.2. Using automatic vulnerability monitoring

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

To check and fix the detected issues:

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

3. You can see detailed information regarding the detected system vulnerabilities. Depending on the issue, to fix a specific vulnerability proceed as follows:
   - If Windows updates are available, click **Install**.
   - If automatic Windows update is disabled, click **Enable**.
   - If an app is outdated, click **Update now** to find a link to the vendor webpage from where you can install the latest version of that app.
   - If a Windows user account has a weak password, click **Change password** to force the user to change the password at the next logon or change the password yourself. For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, $ or @).
   - If the Windows Autorun feature is enabled, click **Fix** to disable it.
   - If the router you have configured has set a weak password, click **Change password** to access its interface from where you can set a strong one.
   - If the network you are connected to has vulnerabilities which may expose your system at risk, click **Change Wi-Fi settings**.

To configure the vulnerability monitoring settings:

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

   Important
   To be automatically notified about system or app vulnerabilities, keep the **Vulnerability** option enabled.

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

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

   Application updates
   Check if apps installed on your system are up-to-date. Outdated apps can be exploited by malicious software, making your PC vulnerable to outside attacks.

User passwords

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

Autoplay

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

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

Wi-Fi security

Check if the wireless home network you are connected to is secure or not, and if it has vulnerabilities. Also, check if the password of your home router is strong enough, and how you can make it safer.

Most unprotected wireless networks are not secure, thus allowing the hackers' prying eyes have access to your private activities.

Note

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

17.3. Wi-Fi Security Advisor

While on the go, working in a coffee shop, or waiting at the airport, connecting to a public wireless network for making payments, checking emails or social network accounts can be the fastest solution. But prying eyes trying to hijack your personal data can be there, watching how the information leaks through the network.

Personal data means the passwords and usernames you use to get access to your online accounts, such as emails, bank accounts, social media accounts, but also the messages you send.

Usually, public wireless networks are more likely to be unsafe since they do not require password at login, and if they do, the password could be made

available to anybody who wants to connect. Moreover, they may be malicious or honeypot networks, representing a target for cyber criminals.

To safeguard you against the perils of unsecured or unencrypted public wireless hotspots, Bitdefender Wi-Fi Security Advisor analyzes how secure a wireless network is, and when necessary, it recommends you to use Bitdefender VPN.

The Bitdefender Wi-Fi Security Advisor gives information about:

- Home Wi-Fi networks
- Public Wi-Fi networks

17.3.1. Turning on or off Wi-Fi Security Advisor notifications

To turn on or off the Wi-Fi Security Advisor notifications:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **VULNERABILITY** pane, click **Settings**.
3. In the **Settings** window, turn on or off the **Wi-Fi security** option.

17.3.2. Configuring Home Wi-Fi network

To start configuring your home network:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **VULNERABILITY** pane, click **Wi-Fi Security**.
3. In the **HOME Wi-Fi** tab, click the **SELECT HOME WI-FI** button.

   A list with the wireless networks you connected to until now is displayed.
4. Point to your home network, and then click **SELECT**.

If a home network is considered unsecured or unsafe, configuration recommendations to improve its security are displayed.

To remove the wireless network you have set as a home network, click the **REMOVE** button.

17.3.3. Public Wi-Fi

While connected to an unsecured or unsafe wireless network, the Public Wi-Fi profile is activated. While running in this profile, Bitdefender Antivirus Plus is set to automatically accomplish the following program settings:

- Advanced Threat Defense is turned on
- The following settings from Online Threat Prevention are turned on:
  - Encrypted web scan
  - Protection against fraud
  - Protection against phishing
- A button that opens Bitdefender Safepay™ is available. In this case, the Hotspot protection for unsecured networks is enabled by default.

17.3.4. Checking information about Wi-Fi networks

To check information about the wireless networks you usually connect to:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **VULNERABILITY** pane, click **Wi-Fi Security**.
3. Depending on the information you need, select one of the two tabs, **HOME Wi-Fi** or **PUBLIC Wi-Fi**.
4. Click **View details** next to the network you want to find more info about.

There are three types of wireless networks filtered by their importance, each type indicated by a specific icon:

Wi-Fi is unsafe - indicates that the security level of the network is low. This means that there is a high risk to use it, and it is not recommended to make payments or check bank accounts without an extra protection. In such situations, we recommend you to use Bitdefender Safepay™ with Hotspot protection for unsecured networks enabled.

Wi-Fi is unsafe - indicates that the security level of the network is moderate. This means that it can have vulnerabilities and it is not recommended to make payments or check bank accounts without an extra protection. In such situations, we recommend you to use Bitdefender Safepay™ with Hotspot protection for unsecured networks enabled.

Wi-Fi is secure - indicates that the network you use is secure. In this case, you can use sensitive data for making online operations.

By clicking the **View details** link in the area of each network, the following details are displayed:

- **Secured** - here you can view if the selected network is secured or not. Unencrypted networks can leave the data you use exposed.

- **Encryption type** - here you can view the encryption type used by the selected network. Some encryption types may not be secure. Therefore, we strongly recommend you to check information about the displayed encryption type to be sure that you are protected while surfing the web.
- **Channel/Frequency** - here you can view the channel frequency used by the selected network.
- **Password strength** - here you can view how strong the password is. Note that the networks that have set weak passwords represent a target to cyber criminals.
- **Type of sign in** - here you can view if the selected network is protected using a password or not. It is highly recommended to connect only to networks that have set strong passwords.
- **Authentication type** - here you can view the authentication type used by the selected network.

Keep the **Notify** option enabled to receive notifications every time your system connects to this network.

18. SAFE FILES

Ransomware is a malicious software that attacks vulnerable systems by locking them, and asks for money to let the user take back the control of his system. This malicious software acts intelligent by displaying false messages to panic the user, urging him to proceed with the asked payment.

The infection can be spread via spam emails, by downloading attachments, or by visiting infected websites and installing malicious apps without letting the user know what is happening on his system.

Ransomware can have one of the following behaviors preventing the user from accessing his system:

- Encrypts sensitive and personal files without giving the possibility of decryption until a ransom is paid by the victim.
- Locks the computer's screen and displays a message asking for money. In this case, no file is encrypted, only the user is forced to proceed with the payment.
- Blocks apps from running.

With Bitdefender Safe Files you can keep protected from ransomware attacks personal files, such as documents, photos or movies.

Note
Advanced Threat Defense and Safe Files are two layers of protection against ransomware. Advanced Threat Defense is the feature that stops ransomware attacks in their tracks to your system's critical areas, while Safe Files makes sure no important file on your computer gets encrypted.

18.1. Turning on or off Safe Files

To turn on or off the Safe Files feature:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **SAFE FILES** pane, turn on or off the switch.

Each time an app will try to access one of the protected file, a Bitdefender pop-up is displayed. You can allow or block the access.

Note
The Safe Files feature is not enabled by default.

18.2. Protect personal files from ransomware attacks

If you want to settle personal files to a shelter:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **SAFE FILES** pane, click **Protected Folders**.
3. The first time you access Protected Folders, you are introduced into the feature. Click **PROTECT MORE FOLDERS** to continue.
4. Select the folder you want to protect, and then click **OK**.

   To add additional folders, click the **Protect more folders** link. Alternatively, drag folders to this window.

By default, the folders Pictures, Videos, Documents, and Music are protected against threat attacks. Personal data stored in online file hosting services such as Box, Dropbox, Google Drive, and OneDrive are also included to the protection environment, provided that their apps are installed on the system.

To avoid system slow down, we recommend you to add utmost 30 folders, or save multiple files in a single folder.

> **Note**
> Custom folders can be protected only for current users. System and app files cannot be added to exceptions.

18.3. Configuring apps access

Those apps that try to change or delete protected files may be flagged as potentially unsafe and added to the Blocked apps' list. If such an app is blocked and you are sure that its behavior is normal, you can allow it by following these steps:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **SAFE FILES** pane, click **Application Access**.
3. The apps that have requested to change files in your protected folders are listed. Turn on the switch next to the app you are sure is safe.

In the same window you can disable ransomware protection for specific apps by turning off the corresponding switch.

If you want to add new apps to the list, click the **Add a new application to the list** link.

18.4. Protection at boot

It is known that many malicious apps are set to run at system startup, a fact which can seriously damage a machine. Bitdefender Boot time protection scans all critical system areas before all files are being loaded, with zero impact on the system.

To disable Protection at boot:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **SAFE FILES** pane, click **Settings**.
3. Turn off **Protection at boot**.

Note
Apps added to exceptions will be scanned as well and treated accordingly.

19. RANSOMWARE REMEDIATION

Bitdefender Ransomware Remediation backs up your files such as documents, pictures, videos, or music to make sure that they are protected from being damaged or lost in case of ransomware encryption. Each time a ransomware attack is detected, Bitdefender will block all processes involved in the attack and start the remediation process. This way, you will be able to recover the content of your entire files without paying for any asked ransom.

19.1. Turning on or off Ransomware Remediation

To turn on or off Ransomware Remediation:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **RANSOMWARE REMEDIATION** pane, turn on or off the switch.

> **Note**
> To ensure that your files are protected against ransomware, we recommend you to keep Ransomware Remediation enabled.

19.2. Turning on or off automatic restore

Automatic Restore makes sure that your files are automatically restored in the event of ransomware encryption.

To turn on or off automatic restore:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **RANSOMWARE REMEDIATION** pane, click **Settings**.
3. Turn on or off the **Automatic restore** switch.

19.3. Viewing files that were automatically restored

When the **Automatic restore** option is enabled, Bitdefender will automatically restore files that were encrypted by a ransomware. This way your can enjoy worry-free computer experience knowing that you files are safe.

To view files that were automatically restored:

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

2. In the **All** tab, select the notification regarding the latest ransomware behavior remediated, and then click **Restored Files**.

   The list with the restored files is displayed. Here you can also view the location where your files have been restored.

19.4. Restoring encrypted files manually

In case you have to manually restore files that were encrypted by a ransomware, follow these steps:

1. Click **Notifications** on the navigation menu on the Bitdefender interface.
2. In the **All** tab, select the notification regarding the latest ransomware behavior detected, and then click **Encrypted Files**.
3. The list with the encrypted files is displayed.

   Click **RECOVER FILES** to continue.
4. In case the entire or a part of the restoring process fails, you have to choose the location where the decrypted files should be saved. Click **RESTORE LOCATION**, and then choose a location on your PC.
5. A confirmation window appears.

   Click **FINISH** to end the restoring process.

Files with the following extensions can be restored in case they get encrypted:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

19.5. Adding applications to exceptions

You can configure exception rules for trusted apps so that the Ransowmare Remediation feature does not block them if they perform ransomware-like actions.

To add apps to the Ransomware Remediation exceptions list:

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

2. In the **RANSOMWARE REMEDIATION** pane, click **Exceptions**.
3. To start adding apps to the list, click **Add a new application to the list**.

20. PASSWORD MANAGER PROTECTION FOR YOUR CREDENTIALS

We use our computers to shop online or pay our bills, to connect to social media platforms or log in with instant messaging apps.

But as everybody knows, it's not always easy to remember the password!

And if we are not careful while browsing online, our private information, such as our email address, our instant messaging ID or our credit card data can be compromised.

To keep your passwords or your personal data on a sheet of paper or in the computer can be dangerous because they can be accessed and used by people who want to steal and use that information. And to remember each password you have set for your online accounts or for your favorite websites is not an easy task.

Therefore, is there a way to make sure that we find our passwords when we need them? And can we rest assured that our secret passwords are always safe?

Password Manager helps you keep track of your passwords, protects your privacy and provides a secure browsing experience.

Using a single master password to access your credentials, Password Manager makes it easy for you to keep your passwords safe in a Wallet.

To offer the best protection for your online activities, Password Manager is integrated with Bitdefender Safepay™ and provides a unified solution for the various ways in which your private data can be compromised.

Password Manager protects the following private information:

- Personal information, such as the email address or the phone number
- Login credentials for the websites
- Bank account information or the credit card number
- Access data to the email accounts
- Passwords for the apps
- Passwords for the Wi-Fi networks

20.1. Create a new Wallet database

Bitdefender Wallet is the place where you can store your personal data. For an easier browser experience, you need to create a Wallet database as follows:

1. Click **Privacy** on the navigation menu on the Bitdefender interface.
2. In the **PASSWORD MANAGER** pane, click **Create new Wallet**.
3. Click **Create new**.
4. Type the required information in the corresponding fields.
   - Wallet label - type a unique name for your Wallet database.
   - Master Password - type a password for your Wallet.
   - Retype Password - retype the password you set.
   - Hint - type a hint to remember the password.
5. Click **CONTINUE**.
6. At this step you can choose to store your information in the cloud. If you select Yes, banking information will remain stored locally on your device. Choose the desired option, then click **CONTINUE**.
7. Select the web browser you want to import credentials from.
8. Click **FINISH**.

20.2. Import an existing database

To import a wallet database stored locally:

1. Click **Privacy** on the navigation menu on the Bitdefender interface.
2. In the **PASSWORD MANAGER** pane, click **Create new Wallet**.
3. Click **FROM TARGET**.
4. Browse to the location on your device where you want to save the wallet database, and then choose a name for it.
5. Click **Open**.
6. Give a name to your Wallet and type in the password assigned when it was created in the first place.
7. Click **IMPORT**.

8. Select the programs you want the Wallet to import credentials from, and then the **FINISH** button.

20.3. Export the Wallet database

To export your Wallet database:

1. Click **Privacy** on the navigation menu on the Bitdefender interface.
2. In the **PASSWORD MANAGER** pane, click **My Wallets**.
3. Click the icon on the desired wallet, and then select **Export**.
4. Search the location of your wallet database and select it (the .db file).
5. Click **Save**.

Note
The Wallet needs to be opened in order for the **Export** option to be available. If the wallet you need to export is locked, click **ACTIVATE WALLET**, and then type in the password assigned when it was created in the first place.

20.4. Synchronize your wallets in the cloud

To turn the wallets synchronization in the cloud on or off:

1. Click **Privacy** on the navigation menu on the Bitdefender interface.
2. In the **PASSWORD MANAGER** pane, click **My Wallets**.
3. Click the icon on the desired wallet, and then select **Settings**.
4. Choose the desired option in the window that appears, then click **Save**.

Note
The Wallet needs to be opened in order for the **Export** option to be available. If the wallet you need to synchronize is locked, click **ACTIVATE WALLET**, and then type in the password assigned when it was created in the first place.

20.5. Manage your Wallet credentials

To manage your passwords:

1. Click **Privacy** on the navigation menu on the Bitdefender interface.
2. In the **PASSWORD MANAGER** pane, click **My Wallets**.

3. Select the desired Wallet database, and then click **ACTIVATE WALLET**.
4. Type the Master password, and then click **OK**.

A new window appears. Select the desired category from the upper part of the window:

- Identity
- Websites
- Online banking
- Emails
- Apps
- Wi-Fi Networks

Adding/ editing the credentials

- To add a new password, choose the desired category from the top, click **+ Add item**, insert the information in the corresponding fields and click the Save button.
- To edit an entry from the table, select it and click the **Edit** button.
- To remove an entry, select it, click the **Delete** button.

20.6. Turning on or off the Password Manager protection

To turn the Password Manager protection on or off:

1. Click **Privacy** on the navigation menu on the Bitdefender interface.
2. In the **PASSWORD MANAGER** pane, turn on or off the switch.

20.7. Managing the Password Manager settings

To configure the master password in detail:

1. Click **Privacy** on the navigation menu on the Bitdefender interface.
2. In the **PASSWORD MANAGER** pane, click **Settings**.
3. Select the **Security Settings** tab.

The following options are available:

- **Ask for my master password when I login to my device** - you will be prompted to insert your master password when you access the device.
- **Ask for my master password when I open my browsers and apps** - you will be prompted to insert your master password when you access a browser or an app.
- **Do not ask me for my master password** - you will not be prompted to insert your master password when you access the computer, a browser or an app.
- **Automatically lock Wallet when I leave my device unattended** - you will be prompted to insert your master password when you return to your device after 15 minutes.

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

Improve your experience

To select the browsers or the apps where you want to integrate Password Manager:

1. Click **Privacy** on the navigation menu on the Bitdefender interface.
2. In the **PASSWORD MANAGER** pane, click **Settings**.
3. Select the **Plugins** tab.

   Check an app to use Password Manager and improve your experience:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay

Configuring the Autofill

The Autofill feature makes it easy for you to connect with your favorite websites or to log in with your online accounts. The first time you enter your login credentials and personal information into your web browser, they are automatically secured into the Wallet.

To configure the **Autofill** settings:

1. Click **Privacy** on the navigation menu on the Bitdefender interface.
2. In the **PASSWORD MANAGER** pane, click **Settings**.
3. Select the **Autofill settings** tab.
4. Configure the following options:
   - **Configure how Password Manager secures your credentials**:
     - **Save credentials automatically in Wallet** - the login credentials and other identifiable information such as your personal and credit card details are automatically saved and updated into the Wallet.
     - **Ask me every time** - you will be asked every time if you want to add your credentials to the Wallet.
     - **Do not save, I will update the information manually** - the credentials can be added only manually into the Wallet.
   - **Autofill login credentials**:
     - **Autofill login credentials every time** - the credentials are inserted automatically into the browser.
   - **Autofill forms**:
     - **Prompt my fill options when I visit a page with forms** - a popup with the fill options will appear every time Bitdefender detects that you want to perform an online payment or to sign up.

Manage the Password Manager information from your browser

You can easily manage the Password Manager details directly from your browser, to have all the important data at hand. The Bitdefender Wallet add-on is supported by the following browsers: Google Chrome, Internet Explorer and Mozilla Firefox, and is also also integrated with Safepay.

To access the Bitdefender Wallet extension, open your web browser, allow the add-on to be installed and click the icon on the toolbar.

The Bitdefender Wallet extension contains the following options:

- Open Wallet - opens the Wallet.
- Lock Wallet - locks the Wallet.

- Web pages - opens a submenu with all the websites logins stored in the Wallet. Click **Add Web Page** to add new websites into the list.
- Fill Forms - opens a submenu containing the information you added for a specific category. From here you can add new data to your Wallet.
- Password Generator - enables you to generate random passwords you can use for new or existing accounts. Click **Show advanced settings** to customize the complexity of the password.
- Settings - opens the Password Manager settings window.
- Report issue - report any issue you encounter with the Bitdefender Password Manager.

21. VPN

The VPN app may be installed from your Bitdefender product and used every time you want to add an extra layer of protection to your connection. The VPN serves as a tunnel between your device and the network you connect to securing your connection, encrypting the data using bank-grade encryption, and hiding your IP address wherever you are. Your traffic is redirected through a separate server; thus making your device almost impossible to be identified through the myriad of other devices that are using our services. Moreover, while connected to the internet via Bitdefender VPN, you are able to access content that is normally restricted in specific areas.

Note
Some countries practice internet censorship and therefore the usage of VPNs on their territory has been banned by law. To avoid legal consequences, a warning message can appear when you try to use the Bitdefender VPN app for the first time. By continuing using the app, you confirm that you are aware of the applicable country regulations and the risks to which you might be exposed.

21.1. Installing VPN

The VPN app can be installed from your Bitdefender interface, as follows:

1. Click **Privacy** on the navigation menu on the Bitdefender interface.
2. In the **VPN** pane, click **Install VPN**.
3. In the window with the description of the VPN app, read the **Subscription agreement**, and then click **INSTALL BITDEFENDER VPN**.

   Wait several moments until the files are downloaded and installed.
4. Click **OPEN BITDEFENDER VPN** to finish the installation process.

Note
Bitdefender VPN requires .Net Framework 4.5.2 or higher to be installed. In case you do not have this package installed, a notification window appears. Click **install .Net Framework** to be redirected to a page from where you can download the newest version of this software.

21.2. Opening VPN

To access the main interface of Bitdefender VPN, use one of the following methods:

- From system tray
  1. Right-click the icon in system tray, and then click **Show**.
- From the Bitdefender interface:
  1. Click **Privacy** on the navigation menu on the Bitdefender interface.
  2. In the **VPN** pane, click **Open VPN**.

21.3. VPN interface

The VPN interface displays the status of the app, connected or disconnected. The server location for users with the free version is automatically set by Bitdefender to the most appropriate server, while premium users have the possibility to change the server location they want to connect to. For more information about VPN subscriptions, refer to "*Subscriptions*" (p. 116).

To connect or disconnect, simply click on the status displayed at the top of the screen, or right-click the system tray icon. The system tray icon displays a green check mark when the VPN is connected, and a red check mark when the VPN is disconnected.

While connected, the elapsed time and the IP address automatically assigned to your device are displayed on the lower part of the interface.

To get access to more options, access the **Menu** area by clicking the ☰ icon in the upper-left side. Here you have the following options:

- **My Account** – details about your Bitdefender account and VPN subscription are displayed. Click **Switch Account** if you want to sign in with another account.
- **Settings** – depending on your needs, you can customize the behavior of your product:
  - receive notifications when the VPN automatically connects or disconnects
  - automatically run the VPN app at Windows startup
  - automatically launch the VPN app when your device connects to unsecured wireless networks

- **Upgrade to Premium** - if you are using the free version, you can upgrade to the premium plan from here.
- **Support** - you are redirected to our Support Center platform from where you can read a helpful article on how to use Bitdefender VPN.
- **About** - information about the installed version is displayed.

21.4. Subscriptions

Bitdefender VPN offers for free a daily 200 MB traffic quota per device to secure your connection every time you need, and connects you automatically to the optimal server location.

To get unlimited traffic and unrestricted access to content worldwide by choosing a server location at your will, upgrade to the premium version.

You can upgrade to the Bitdefender Premium VPN version anytime by clicking the **GET UNLIMITED TRAFFIC** button available in the product interface.

The Bitdefender Premium VPN subscription is independent from the Bitdefender Antivirus Plus subscription, meaning you will be able to use it for its entire availability, regardless of the state of the security solution subscription. In case the Bitdefender Premium VPN subscription expires, but the one for Bitdefender Antivirus Plus is still active, you will be reverted to the free plan.

Bitdefender VPN is a cross-platform product, available in Bitdefender products compatible with Windows, macOS, Android and iOS. Once you upgrade to the premium plan, you will be able to use your subscription on all products, provided that you login with the same Bitdefender account.

22. SAFEPAY SECURITY FOR ONLINE TRANSACTIONS

The computer is quickly becoming the main tool for shopping and banking. Paying bills, transferring money, buying pretty much anything you can imagine has never been quicker or easier.

This involves sending personal information, account and credit card data, passwords and other types of private information over the internet, in other words exactly the type of information flow that cyber-criminals are very interested to tap into. Hackers are relentless in their efforts to steal this information, so you can never be too careful about securing online transactions.

Bitdefender Safepay™ is first of all a protected browser, a sealed environment that is designed to keep your online banking, e-shopping and any other type of online transaction private and secure.

For the best privacy protection, Bitdefender Password Manager has been integrated into Bitdefender Safepay™ to secure your credentials whenever you want to access private online locations. For more information, refer to "*Password Manager protection for your credentials*" (p. 107).

Bitdefender Safepay™ offers the following features:

- It blocks access to your desktop and any attempt to take snapshots of your screen.
- It protects your secret passwords while browsing online with Password Manager.
- It comes with a virtual keyboard which, when used, makes it impossible for hackers to read your keystrokes.
- It is completely independent from your other browsers.
- It comes with built-in hotspot protection to be used when your computer is connected to unsecured Wi-fi networks.
- It supports bookmarks and allows you to navigate between your favorite banking/shopping sites.
- It is not limited to banking and e-shopping. Any website can be opened in Bitdefender Safepay™.

22.1. Using Bitdefender Safepay™

By default, Bitdefender detects when you navigate to an online banking site or online shop in any browser on your computer and prompts you to launch it in Bitdefender Safepay™.

To access the main interface of Bitdefender Safepay™, use one of the following methods:

- From the Bitdefender interface:
  1. Click **Privacy** on the navigation menu on the Bitdefender interface.
  2. In the **Safepay** pane, click **Open Safepay**.
- From Windows:
  - In **Windows 7**:
    1. Click **Start** and go to **All Programs**.
    2. Click **Bitdefender**.
    3. Click **Bitdefender Safepay™**.
  - In **Windows 8 and Windows 8.1**:

    Locate Bitdefender Safepay™ from the Windows Start screen (for example, you can start typing "Bitdefender Safepay™" directly in the Start screen) and then click the icon.
  - In **Windows 10**:

    Type "Bitdefender Safepay™" in the search box from the taskbar and click its icon.

> **Note**
> If the Adobe Flash Player plugin is not installed or is outdated, a Bitdefender message will be displayed. Click the corresponding button to continue.
> After the installation process is completed, you will have to manually reopen the Bitdefender Safepay™ browser to continue your work.

If you are used to web browsers, you will have no trouble using Bitdefender Safepay™ - it looks and behaves like a regular browser:

- enter URLs you want to go to in the address bar.
- add tabs to visit multiple websites in the Bitdefender Safepay™ window by clicking +.

- navigate back and forward and refresh pages using respectively.
- access Bitdefender Safepay™ settings by clicking and choosing **Settings**.
- protect your passwords with Password Manager by clicking .
- manage your bookmarks by clicking next to the address bar.
- open the virtual keyboard by clicking .
- increase or decrease the browser size by pressing simultaneously **Ctrl** and the **+/-** keys in the numeric keypad.
- view information about your Bitdefender product by clicking and choosing **About**.
- print important information by clicking .

Note
To switch between Bitdefender Safepay™ and Windows desktop, press the **Alt+Tab** keys, or click the **Switch to Desktop** option on the upper left side of the window.

22.2. Configuring settings

Click and choose **Settings** to configure Bitdefender Safepay™:

Domains list

Choose how Bitdefender Safepay™ will behave when you visit websites from specific domains in your regular web browser by adding them to the domains list and selecting the behavior for each one:

- Automatically open in Bitdefender Safepay™.
- Have Bitdefender prompt you for action each time.
- Never use Bitdefender Safepay™ when visiting a page from the domain in a regular browser.

Blocking pop-ups

You can choose to block pop-ups by clicking the corresponding switch.

You can also create a list of websites to allow pop-ups from. The list should contain only websites you fully trust.

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

To remove a website from the list, select the X corresponding to the desired entry.

Manage Plugins
You can choose whether you wish to enable or disable specific plugins in Bitdefender Safepay™.

Manage certificates
You can import certificates from your system to a certificate store.

Select **Import certificates** and follow the wizard to use the certificates in Bitdefender Safepay™.

Automatically launch Virtual Keyboard at password fields
The Virtual Keyboard will automatically appear when a password field is selected.

Use the corresponding switch to enable or disable the feature.

Ask for confirmation before printing
Enable this option if you want to give your confirmation before the printing process starts.

22.3. Managing bookmarks

If you disabled the automatic detection of some or all websites, or Bitdefender simply doesn't detect certain websites, you can add bookmarks to Bitdefender Safepay™ so that you can easily launch favorite websites in the future.

Follow these steps to add a URL to Bitdefender Safepay™ bookmarks:

1. Click the icon next to the address bar to open the Bookmarks page.

   Note
   The Bookmarks page is opened by default when you start Bitdefender Safepay™.

2. Click the **+** button to add a new bookmark.
3. Type the URL and the title of the bookmark and click **Create**. Check the **Automatically open in Safepay** option if you want the bookmarked page to open with Bitdefender Safepay™ each time you access it. The URL is also added to the Domains list on the settings page.

22.4. Turning off Safepay notifications

When a banking site is detected, the Bitdefender product is set up to notify you through a pop-up window.

To turn off the Safepay notifications:

1. Click **Privacy** on the navigation menu on the Bitdefender interface.
2. In the **Safepay** pane, click **Settings**.
3. Turn off **Safepay notifications**.

22.5. Using VPN with Safepay

To make online payments in a safe environment while being connected to unsecured networks, the Bitdefender product may be set up to automatically launch the VPN app in the same time with Safepay.

To start using the VPN app together with Safepay:

1. Click **Privacy** on the navigation menu on the Bitdefender interface.
2. In the **Safepay** pane, click **Settings**.
3. Turn on **Use VPN with Safepay**.

23. DATA PROTECTION

23.1. Deleting files permanently

When you delete a file, it can no longer be accessed through normal means. However, the file continues to be stored on the hard disk until it is overwritten when copying new files.

The Bitdefender File Shredder helps you permanently delete data by physically removing it from your hard disk.

You can quickly shred files or folders from your computer using the Windows contextual menu by following these steps:

1. Right-click the file or folder you want to permanently delete.
2. Select **Bitdefender** > **File Shredder** in the context menu that appears.
3. Click **DELETE PERMANENTLY**, and then confirm that you wish to continue with the process.

   Wait for Bitdefender to finish shredding the files.
4. The results are displayed. Click **FINISH** to exit the wizard.

Alternatively, you can shred files from the Bitdefender interface, as follows:

1. Click **Privacy** on the navigation menu on the Bitdefender interface.
2. In the **DATA PROTECTION** pane, click **File Shredder**.
3. Follow the File Shredder wizard:
   a. Click the **ADD FOLDERS** button to add the files or folders you want to be permanently removed.

      Alternatively, drag these files or folders to this window.
   b. Click **DELETE PERMANENTLY**, and then confirm that you wish to continue with the process.

      Wait for Bitdefender to finish shredding the files.
   c. **Results Summary**

      The results are displayed. Click **FINISH** to exit the wizard.

24. USB IMMUNIZER

The Autorun feature built into Windows operating systems is a very useful tool that allows computers to automatically execute a file from media connected to it. For example, software installations can start automatically when a CD is inserted into the optical drive.

Unfortunately, this feature can also be used by threats to automatically launch and infiltrate your computer from rewritable media such as USB flash drives and memory cards connected through card readers. Numerous Autorun based attacks have been created in recent years.

With USB Immunizer you can prevent any NTFS, FAT32 or FAT formatted flash drive from automatically executing threats ever again. Once an USB device is immunized, threats can no longer configure it to run a certain app when the device is connected to a computer running Windows.

To immunize an USB device:

1. Connect the flash drive to your computer.
2. Browse your computer to locate the removable storage device and right-click its icon.
3. In the contextual menu, point to **Bitdefender** and select **Immunize this drive**.

> **Note**
> If the drive has already been immunized, the message **The USB device is protected against autorun-based threat** will appear instead of the Immunize option.

To prevent your computer from launching threats from unimmunized USB devices, disable the media autorun feature. For more information, refer to "*Using automatic vulnerability monitoring*" (p. 95).

SYSTEM OPTIMIZATION

25. PROFILES

Daily job activities, watching movies or playing games may cause system slow down, especially if they are running simultaneously with Windows update processes and maintenance tasks. With Bitdefender, you can now choose and apply your preferred profile, which makes system adjustments suited to increase the performance of specific installed apps.

Bitdefender provides the following profiles:

- Work Profile
- Movie Profile
- Game Profile
- Public Wi-Fi Profile
- Battery Mode Profile

If you decide to not use **Profiles**, a default profile called **Standard** is enabled and it brings no optimization to your system.

According to your activity, the following product settings are applied when Work, Movie or Game profiles are activated:

- All Bitdefender alerts and pop-ups are disabled.
- Automatic Update is postponed.
- Scheduled scans are postponed.
- Search Advisor is disabled.
- Special offers notifications are disabled.

According to your activity, the following system settings are applied when Work, Movie or Game profiles are activated:

- Windows Automatic Updates are postponed.
- Windows alerts and pop-ups are disabled.
- Unnecessary background programs are suspended.
- Visual effects are adjusted for best performance.
- Maintenance tasks are postponed.
- Power plan settings are adjusted.

While running in the Public Wi-Fi profile, Bitdefender Antivirus Plus is set to automatically accomplish the following program settings:

- Advanced Threat Defense is turned on
- The following settings from Online Threat Prevention are turned on:
  - Encrypted web scan
  - Protection against fraud
  - Protection against phishing

25.1. Work Profile

Running multiple tasks at work, such as sending emails, having a video communication with your distant colleagues or working with design apps may affect your system performance. Work Profile has been designed to help you improve your work efficiency, by turning off some of your background services and maintenance tasks.

Configuring Work Profile

To configure the actions to be taken while in Work Profile:

1. Click **Settings** on the navigation menu on the Bitdefender interface.
2. Select the **Profiles** tab.
3. Click the **CONFIGURE** button from the Work Profile area.
4. Choose the system adjustments you would like to be applied by checking the following options:
   - Boost performance on work apps
   - Optimize product settings for Work profile
   - Postpone background programs and maintenance tasks
   - Postpone Windows Automatic Updates
5. Click **SAVE** to save the changes and close the window.

Manually adding apps to the Work Profile list

If Bitdefender does not automatically enter Work Profile when you launch a certain work app, you can manually add the app to the **Work application list**.

To manually add apps to the Work application list in Work Profile:

1. Click **Settings** on the navigation menu on the Bitdefender interface.
2. Select the **Profiles** tab.
3. Click the **CONFIGURE** button from the Work Profile area.
4. In the **Work profile settings** window, click **Applications list**.
5. Click **ADD**.

   A new window appears. Browse to the app's executable file, select it and click **OK** to add it to the list.

25.2. Movie Profile

Displaying high quality video content, such as high definition movies, requires significant system resources. Movie Profile adjusts system and product settings so you can enjoy an uninterrupted and seamless movie experience.

Configuring Movie Profile

To configure the actions to be taken while in Movie Profile:

1. Click **Settings** on the navigation menu on the Bitdefender interface.
2. Select the **Profiles** tab.
3. Click the **CONFIGURE** button from the Movie Profile area.
4. Choose the system adjustments you would like to be applied by checking the following options:
   - Boost performance on video players
   - Optimize product settings for Movie profile
   - Postpone background programs and maintenance tasks
   - Postpone Windows Automatic Updates
   - Adjust power plan settings for movies
5. Click **SAVE** to save the changes and close the window.

Manually adding video players to the Movie Profile list

If Bitdefender does not automatically enter Movie Profile when you launch a certain video player app, you can manually add the app to the **Movie application list**.

To manually add video players to the Movie application list in Movie Profile:

1. Click **Settings** on the navigation menu on the Bitdefender interface.
2. Select the **Profiles** tab.
3. Click the **CONFIGURE** button from the Movie Profile area.
4. In the **Movie profile settings** window, click **Players list**.
5. Click **ADD**.

   A new window appears. Browse to the app's executable file, select it and click **OK** to add it to the list.

25.3. Game Profile

Enjoying an uninterrupted gaming experience is all about reducing system load and diminishing slowdowns. By using behavioral heuristics along with a list of known games, Bitdefender can automatically detect running games and optimize your system resources so that you can enjoy your gaming break.

Configuring Game Profile

To configure the actions to be taken while in Game Profile:

1. Click **Settings** on the navigation menu on the Bitdefender interface.
2. Select the **Profiles** tab.
3. Click the **CONFIGURE** button from the Game Profile area.
4. Choose the system adjustments you would like to be applied by checking the following options:
   - Boost performance on games
   - Optimize product settings for Game profile
   - Postpone background programs and maintenance tasks
   - Postpone Windows Automatic Updates

- Adjust power plan settings for games

5. Click **SAVE** to save the changes and close the window.

Manually adding games to the Game list

If Bitdefender does not automatically enter Game Profile when you launch a certain game or app, you can manually add the app to the **Game application list**.

To manually add games to the Game application list in Game Profile:

1. Click **Settings** on the navigation menu on the Bitdefender interface.
2. Select the **Profiles** tab.
3. Click the **CONFIGURE** button from the Game Profile area.
4. In the **Game profile settings** window, click **Games list**.
5. Click **ADD**.

   A new window appears. Browse to the game's executable file, select it and click **OK** to add it to the list.

25.4. Public Wi-Fi Profile

Sending emails, typing sensitive credentials or shopping online while connected to unsafe wireless networks can expose your personal data to risk. Public Wi-Fi Profile adjusts product settings to give you the possibility to make payments online and use sensitive information in a protected environment.

Configuring Public Wi-Fi profile

To configure Bitdefender to apply product settings while connected to an unsafe wireless network:

1. Click **Settings** on the navigation menu on the Bitdefender interface.
2. Select the **Profiles** tab.
3. Click the **CONFIGURE** button from the Public Wi-Fi Profile area.
4. Let the **Adjusts product settings to boost protection when connected to an unsafe public Wi-Fi network** check box enabled.
5. Click **Save**.

25.5. Battery Mode Profile

Battery Mode profile is specially designed for laptop and tablet users. Its purpose is to minimize both system and Bitdefender impact on power consumption when the battery charge level is lower than the default one or the one you select.

Configuring Battery Mode Profile

To configure the Battery Mode profile:

1. Click **Settings** on the navigation menu on the Bitdefender interface.
2. Select the **Profiles** tab.
3. Click the **CONFIGURE** button from the Battery Mode Profile area.
4. Choose the system adjustments to be applied by checking the following options:
   - Optimize product settings for Battery mode.
   - Postpone background programs and maintenance tasks.
   - Postpone Windows Automatic Updates.
   - Adjust power plan settings for Battery mode.
   - Disable external devices and network ports.
5. Click **SAVE** to save the changes and close the window.

Type a valid value in the spin box or select one using the up and down arrow keys to specify when the system should start operating in Battery Mode. By default, the mode is activated when the battery charge level drops below 30%.

The following product settings are applied when Bitdefender operates in Battery Mode profile:

- Bitdefender Automatic Update is postponed.
- Scheduled scans are postponed.
- Security Widget is turned off.

Bitdefender detects when your laptop has switched to battery power and based on the battery charge level it automatically enters Battery Mode.

Likewise, Bitdefender automatically exits Battery Mode when it detects the laptop is no longer running on battery.

25.6. Real-time optimization

Bitdefender Real-time optimization is a plugin that improves your system performance silently, in the background, making sure that you are not interrupted while you are in a profile mode. Depending on the CPU load, the plugin monitors all processes, focusing on those that take up a higher load, to adjust them to your needs.

To turn on or off Real-time optimization:

1. Click **Settings** on the navigation menu on the Bitdefender interface.
2. Select the **Profiles** tab.
3. Scroll down until you see the Real-time optimization option, and then use the corresponding switch to turn it on or off.

TROUBLESHOOTING

26. 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. 133)
- "*Scan doesn't start*" (p. 134)
- "*I can no longer use an app*" (p. 137)
- "*What to do when Bitdefender blocks a safe website or online app*" (p. 137)
- "*What to do if Bitdefender detects a safe app as ransomware*" (p. 138)
- "*How to update Bitdefender on a slow internet connection*" (p. 138)
- "*Bitdefender services are not responding*" (p. 139)
- "*The Autofill feature in my Wallet doesn't work*" (p. 140)
- "*Bitdefender removal failed*" (p. 141)
- "*My system doesn't boot up after installing Bitdefender*" (p. 142)

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. 155).

26.1. 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. 66).

- **The Minimum System Requirements for running Bitdefender are not met.**

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

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

  Any computer 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 computer'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 **System Scan**.
  3. Follow the wizard steps.

26.2. 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 Plus** 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 Plus** 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 Plus** 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. 66).
  2. Reinstall Bitdefender:

- In **Windows 7**:
  a. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
  b. Find **Bitdefender Antivirus Plus** 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 Plus** 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 Plus** 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. 155).

26.3. 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 **Settings**.
3. In the **Exceptions** window, click **Add applications to exceptions**.
4. Find and select the app you want to be excepted, and then click **OK**.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 155).

26.4. What to do when Bitdefender blocks a safe website or online app

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 safe website or online app as unsafe, which will cause Bitdefender HTTP traffic scanning to block them incorrectly.

Should the same page or 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 **Exceptions**.
3. Provide the address of the blocked website or online app in the corresponding field and click **ADD**.
4. Click **SAVE** to save the changes and close the window.

Only websites 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. 155).

26.5. What to do if Bitdefender detects a safe app as ransomware

Ransomware is a malicious program that tries to make money from users by locking their vulnerable systems. To keep your system safe from unfortunate situations, Bitdefender gives you the possibility to indemnify personal files.

When an app tries to change or delete one of your protected files, it will be considered as unsafe and Bitdefender will block its functionality.

In case such an app is added to the untrusted apps' list and you are sure that it is safe to use it, follow these steps:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **SAFE FILES** pane, click **Application Access**.
3. The apps that have requested to change files in your protected folders are listed. Click the **Allow** switch next to the app you are sure is safe.

26.6. 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.

26.7. 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 computer at the same time with Bitdefender.

To troubleshoot this error, try these solutions:

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

For more information, refer to "*How do I remove other security solutions?*" (p. 66).

If the error persists, please contact our support representatives for help as described in section "*Asking for help*" (p. 155).

26.8. The Autofill feature in my Wallet doesn't work

You have saved your online credentials in your Bitdefender Password Manager and you noticed that the autofill is not working. Usually, this issue appears when the Bitdefender Wallet extension is not installed in your browser.

To fix this situation, follow these steps:

- In **Internet Explorer:**
  1. Open Internet Explorer.
  2. Click Tools.
  3. Click Manage add-ons.
  4. Click Toolbars and Extensions.
  5. Point to **Bitdefender Wallet** and click **Enable**.
- In **Mozilla Firefox:**
  1. Open Mozilla Firefox.
  2. Click Tools.
  3. Click Add-ons.
  4. Click Extensions.
  5. Point to **Bitdefender Wallet** and click **Enable**.
- In **Google Chrome:**
  1. Open Google Chrome.
  2. Go to the Menu icon.
  3. Click More Tools.
  4. Click Extensions.
  5. Point to **Bitdefender Wallet** and click **Enable**.

Note
The add-on will be enabled after you restart your web browser.

Now check if the autofill feature in Wallet works for your online accounts.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 155).

26.9. 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 Plus** 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 Plus** 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 Plus** 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.

26.10. 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. 67).
  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 Plus** 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 Plus** 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 Plus** 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. 67).
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. 67).
2. Use the System Restore option from Windows to restore the computer 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. 155).

27. 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.

- "*Bitdefender Rescue Mode (Rescue Environment in Windows 10)*" (p. 145)
- "*What to do when Bitdefender finds threats on your computer?*" (p. 149)
- "*How do I clean a threat in an archive?*" (p. 150)
- "*How do I clean a threat in an email archive?*" (p. 151)
- "*What to do if I suspect a file as being dangerous?*" (p. 152)
- "*What are the password-protected files in the scan log?*" (p. 152)
- "*What are the skipped items in the scan log?*" (p. 153)
- "*What are the over-compressed files in the scan log?*" (p. 153)
- "*Why did Bitdefender automatically delete an infected file?*" (p. 153)

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. 155).

27.1. Bitdefender Rescue Mode (Rescue Environment in Windows 10)

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

Once Bitdefender Antivirus Plus is installed on **Windows 7, Windows 8 and Windows 8.1** and the Bitdefender Rescue Mode Image file downloaded, Rescue Mode can be used even if you are no longer able to boot into Windows.

In Windows 10, Bitdefender Rescue Environment is integrated with Windows RE, meaning there is no need to download any Rescue Mode Image on this operating system, and the feature cannot be used if there are startup

problems. To clean the system before Windows services are loaded, we recommend using Bitdefender Rescue CD.

Bitdefender Rescue CD is a free tool that scans and cleans your computer whenever you suspect a threat is affecting its operation. Useful articles containing details on how to create and use it are available on the Bitdefender Support Center platform at https://www.bitdefender.com/support/consumer.html.

Downloading the Bitdefender Rescue Mode Image

To be able to use Rescue Mode in **Windows 7, Windows 8 and Windows 8.1**, first you have to download its image file as follows:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **ANTIVIRUS** pane, click **Rescue Mode**.
3. Click **Yes** in the confirmation window that appears to reboot your computer.

   Wait for the Bitdefender Rescue Mode Image file to be downloaded from the Bitdefender servers. As soon as the downloading process is finished, the computer will restart.

   A menu appears prompting you to select an operating system. At this step you can choose to start your system in Rescue Mode or in normal mode.

> **Note**
> Due to the integration with Windows Recovery Environment in **Windows 10**, there is no need to download any Rescue Mode Image on this operating system.

Starting your system in Rescue Mode in Windows 7, Windows 8 and Windows 8.1

You can enter Rescue Mode in one of two ways:

From the Bitdefender interface

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

3. Click **Yes** in the confirmation window that appears to reboot your computer.
4. After the computer restarts, a menu appears prompting you to select an operating system. Choose **Bitdefender Rescue Mode** to boot into a Bitdefender environment from where you can clean up your Windows partition.
5. If prompted, press **Enter** and select the screen resolution closest to the one you normally use. Then press **Enter** again.

   Bitdefender Rescue Mode loads in a few moments.

Boot your computer directly into Rescue Mode

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

- In **Windows 7**:
  1. Press the **F8** key until the **Advanced Boot Options** screen appears.
  2. Use the arrow keys to select Bitdefender Rescue Mode, and then press **Enter**.

     Bitdefender Rescue Mode will load in a few moments.
- In **Windows 8 and Windows 8.1**:
  1. Press the **Shift** key until the **Advanced Startup Options** screen appears.
  2. Select the **Use another operating system** option, and then Bitdefender Rescue Mode.

     Bitdefender Rescue Mode will load in a few moments.

Note
It is possible to load your computer in Rescue Mode only if the Rescue Mode Image file has been previous downloaded as described in "Downloading the Bitdefender Rescue Mode Image" (p. 146).

Starting your system in Rescue Environment in Windows 10

You can enter Rescue Environment only from your Bitdefender product, as follows:

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

2. In the **ANTIVIRUS** pane, click **Rescue Environment**.
3. Click **Reboot** in the window that appears.

   Bitdefender Rescue Environment loads in a few moments.

Scanning your system in Rescue Mode (Rescue Environment in Windows 10)

To scan your system in Rescue Mode (Rescue Environment):

- In **Windows 7, Windows 8 and Windows 8.1**:
  1. Enter Rescue Mode, as described in "Starting your system in Rescue Mode in Windows 7, Windows 8 and Windows 8.1" (p. 146).
  2. The Bitdefender logo will appear and the security solution engines will start to be copied.
  3. A welcome window will then appear. Click **Continue**.
  4. An update of the threat information database is started.
  5. After the update is completed, the Bitdefender On-demand Antivirus Scanner window appears.
  6. Click **Scan Now**, select the scan target in the window that appears, and then click **Open** to start scanning.

     It is recommended to scan your entire Windows partition.

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

  7. Wait for the scan to complete. If any threat is detected, follow the instructions to remove it.
  8. To exit Rescue Mode, right-click in an empty area of the desktop, select **Exit** in the menu that appears, and then choose whether to reboot or shut down the computer.
- In **Windows 10**:
  1. Enter Rescue Environment, as described in "Starting your system in Rescue Environment in Windows 10" (p. 147).

2. The Bitdefender scanning process starts automatically as soon as the system is loaded in Rescue Environment.
3. Wait for the scan to complete. If any threat is detected, follow the instructions to remove it.
4. To exit Rescue Environment, click the **CLOSE** button in the window with the scan results.

27.2. What to do when Bitdefender finds threats on your computer?

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

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

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 **Settings**.
   c. In the **Shield** 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. 65).

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. 67).
2. Display hidden objects in Windows. To find out how to do this, refer to "*How do I display hidden objects in Windows?*" (p. 65).
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. 155).

27.3. 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 **Settings**.

c. In the **Shield** 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. 155).

27.4. 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 **Settings**.
   c. In the **Shield** 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. 155).

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

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

To make sure your system is protected:

1. Run a **System Scan** with Bitdefender. To find out how to do this, refer to "*How do I scan my system?*" (p. 54).
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. 155).

27.6. 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 computer 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.

27.7. 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.

27.8. 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.

27.9. 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

28. 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. 133) 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 Plus" (p. 155)
- "Contact us through our online Support Center" (p. 156)

Contact us directly from Bitdefender Antivirus Plus

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

Follow these steps:

1. Click **Support** on the navigation menu on 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.
   - **CONTACT SUPPORT**

     Click **CONTACT SUPPORT** to launch the Bitdefender Support Tool and contact the Customer Care Department.

     a. Complete the submission form with the necessary data:

        i. Select the type of issue you experienced.

        ii. Type a description of the issue you encountered.

iii. Click **TRY TO REPRODUCE THIS ISSUE** in case you are encountering a product issue. Reproduce the issue, and then click **FINISH** in the REPRODUCING THE ISSUE frame.

iv. Click **CONFIRM TICKET**.

b. Continue completing the submission form with the necessary data:

i. Type your full name.

ii. Type your email address.

iii. Select the agreement check box.

iv. Click **CREATE DEBUG PACKAGE**.

Wait for a few moments while Bitdefender gathers product related information. This information will help our engineers find a solution to your problem.

c. Click **CLOSE** to exit the wizard. You will be contacted as soon as possible by one of our representatives.

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.

29. 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.

29.1. 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.

29.2. 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 computer or if you have questions about the way it works, post your problem or question on the forum.

Bitdefender support technicians monitor the forum for new posts 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.

29.3. HOTforSecurity Portal

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

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.

30. 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.

30.1. 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

30.2. 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.

30.3. 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, 15A Orhideelor Street, Sector 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.

Command line

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

Cookie

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

Disk drive

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

A hard disk drive reads and writes hard disks.

A floppy drive accesses floppy disks.

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

Download

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

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.

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.

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.