Bitdefender®
ANTIVIRUS FOR MAC

USER'S GUIDE

Mac

Bitdefender Antivirus for Mac

User's Guide

Publication date 11/24/2022

Legal Notice

Bitdefender

Table of Contents

ABOUT THIS GUIDE

Purpose and Intended Audience

This guide is intended to all Macintosh users who have chosen Bitdefender Antivirus for Mac as a security solution for their computers. The information presented in this book is suitable not only for computer literates, it is accessible to everyone who is able to work under Macintosh.

You will find out how to configure and use Bitdefender Antivirus for Mac to protect yourself against threats and other malicious software. You will learn how to get the best out of your Bitdefender.

We wish you a pleasant and useful lecture.

How to Use This Guide

This guide is organized around several major topics:

Getting Started (page 10)

Get started with Bitdefender Antivirus for Mac and its user interface.

Protecting against Malicious Software (page 14)

Learn how to use Bitdefender Antivirus for Mac to protect yourself against malicious software.

Configuring Preferences (page 33)

Learn more about the Bitdefender Antivirus for Mac preferences.

Getting Help (page 49)

Where to look and where to ask for help if something unexpected appears.

Conventions used in This Guide

Typographical Conventions

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

Appearance	Description
`sample syntax`	Syntax samples are printed with `monospaced` characters.
https://www.bitdefender.com	The URL link is pointing to some external location, on http or ftp servers.
documentation@bitdefender.com	Email addresses are inserted in the text for contact information.
About this Guide (page 1)	This is an internal link, towards some location inside the document.
`filename`	File and directories are printed using `monospaced` font.
option	All the product options are printed using **bold** characters.
keyword	Important keywords or phrases are highlighted using **bold** characters.

Admonitions

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

Note

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

Important

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

Warning

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

Request for Comments

We invite you to help us improve the book. We have tested and verified all of the information to the best of our ability. Please write to tell us about any flaws you find in this book or how you think it could be improved, to help us provide you with the best documentation possible.

Let us know by sending an email to documentation@bitdefender.com. Write all of your documentation-related emails in English so that we can process them efficiently.

1. WHAT IS BITDEFENDER ANTIVIRUS FOR MAC

Bitdefender Antivirus for Mac is a powerful antivirus scanner, which can detect and remove all kinds of malicious software ("threats"), including:

- ransomware
- adware
- viruses
- spyware
- Trojans
- keyloggers
- worms

This app detects and removes not only Mac threats, but also Windows threats, thus preventing you from accidentally sending infected files to your family, friends and colleagues using PCs.

2. INSTALLATION AND REMOVAL

This chapter includes the following topics:

2.1. System Requirements

You may install Bitdefender Antivirus for Mac on Macintosh computers running OS X Yosemite (10.10) or newer versions.

Your Mac must also have minimum 1 GB available hard disk space.

An internet connection is required to register and update Bitdefender Antivirus for Mac.

Note
Bitdefender Anti-tracker and Bitdefender VPN can only be installed on systems running macOS 10.12 or newer versions.

How to find out your macOS version and hardware information about your Mac
Click the Apple icon in the upper-left corner of the screen and choose About **This Mac**. In the window that appears you can see the version of your operating system and other useful information. Click **System Report** for detailed hardware information.

2.2. Installing Bitdefender Antivirus for Mac

The Bitdefender Antivirus for Mac app can be installed from your Bitdefender account as follows:

1. Sign in as an administrator.
2. Go to: https://central.bitdefender.com.
3. Sign in to your Bitdefender account using your email address and password.
4. Select the **My Devices** panel, and then click **INSTALL PROTECTION**.
5. Choose one of the two available options:

- **Protect this device**
  a. Select this option, and then select the owner of the device. If the device belongs to someone else, click the corresponding button.
  b. Save the installation file.
- **Protect other devices**
  a. Select this option, and then select the owner of the device. If the device belongs to someone else, click the corresponding button.
  b. Click **SEND DOWNLOAD LINK**.
  c. 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.
  d. 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.

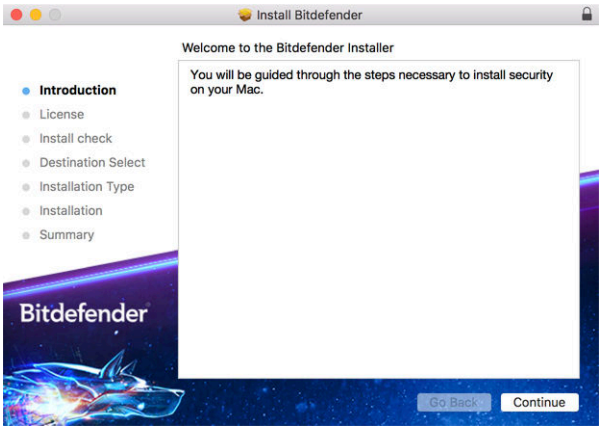
6. Run the Bitdefender product you have downloaded.
7. Complete the installation steps.

2.2.1. Installation process

To install Bitdefender Antivirus for Mac:

1. Click the downloaded file. This will launch the installer, which will guide you through the installation process.
2. Follow the installation wizard.

Step 1 - Welcome Window



Click **Continue**.

Step 2 - Read the Subscription Agreement

Before continuing 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 for Mac.

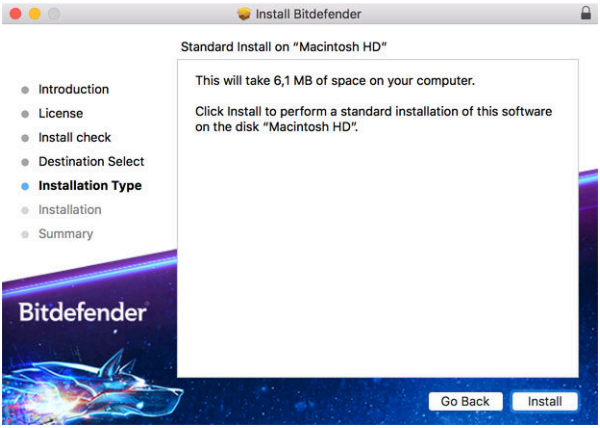
From this window you can also select the language you want to install the product in.

Click **Continue**, and then click **Agree**.

Important

If you do not agree to these terms, click **Continue**, and then click **Disagree** to cancel the installation and quit the installer.

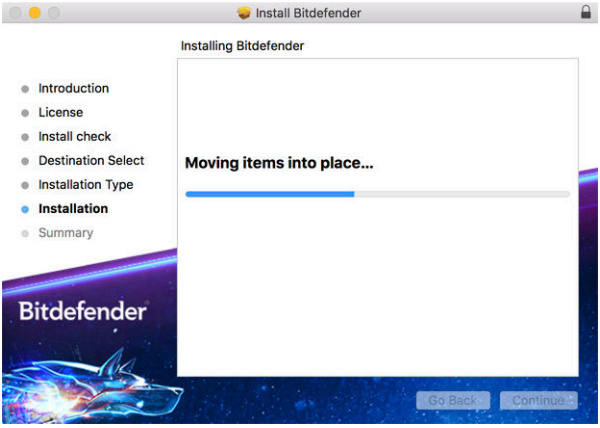
Step 3 - Start Installation



Bitdefender Antivirus for Mac will be installed in `Macintosh HD/Library/Bitdefender`. The installation path cannot be changed.

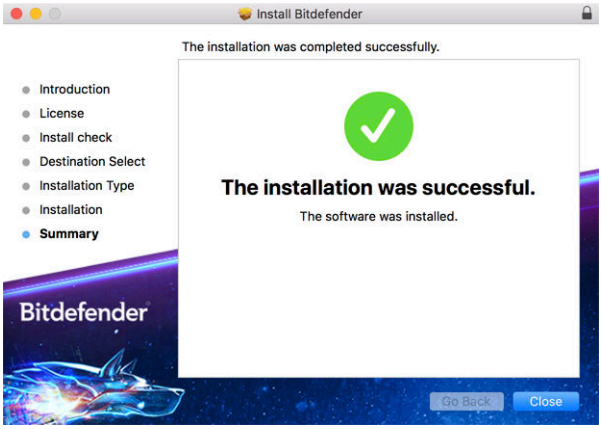
Click **Install** to start the installation.

Step 4 - Installing Bitdefender Antivirus for Mac



Wait until the installation is completed, and then click **Continue**.

Step 5 - Finish



Click **Close** to close the installer window.

The installation process is now complete.

Important

- If you are installing Bitdefender Antivirus for Mac on macOS High Sierra 10.13.0 or a newer version, the **System Extension Blocked** notification appears. This notification informs you that the extensions signed by Bitdefender have been blocked and must be manually enabled. Click OK to continue. In the Bitdefender Antivirus for Mac window that appears, click the **Security & Privacy** link. Click **Allow** in the lower part of the window, or select the Bitdefender SRL from the list, and then click **OK**.
- If you are installing Bitdefender Antivirus for Mac on macOS Mojave 10.14 or a newer version, a new window will be displayed, informing you that you have to **Grant Bitdefender Full Disk Access** and **Allow Bitdefender to load**. Follow the on-screen instructions to properly configure the product.

2.3. Removing Bitdefender Antivirus for Mac

Being a complex app, Bitdefender Antivirus for Mac cannot be removed in the normal way, by dragging the app icon from the *Applications* folder to the Trash.

To remove Bitdefender Antivirus for Mac, follow these steps:

1. Open a **Finder** window, and then go to the *Applications* folder.
2. Open the Bitdefender folder in `Applications`, and then double-click **BitdefenderUninstaller**.
3. Select the preferred uninstall option.

   > **Note**
   > If you're trying to remove just the Bitdefender VPN app select **Uninstall VPN** only.

4. Click **Uninstall** and wait for the process to complete.
5. Click **Close** to finish.

   > **Important**
   > If there is an error, you can contact Bitdefender Customer Care as described in Asking for Help (page 49).

3. GETTING STARTED

This chapter includes the following topics:

3.1. Opening Bitdefender Antivirus for Mac

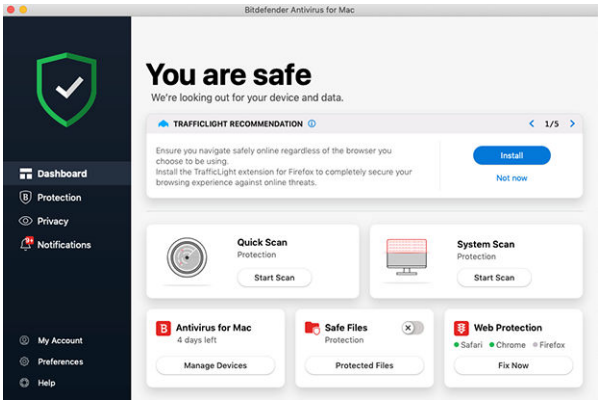
You have several ways to open Bitdefender Antivirus for Mac.

- Click the Bitdefender Antivirus for Mac icon in the Launchpad.
- Click the icon in the menu bar and choose **Open Antivirus interface**.
- Open a Finder window, go to Applications and double-click the icon **Bitdefender Antivirus for Mac**.

> **Important**
> The first time you open Bitdefender Antivirus for Mac on macOS Mojave 10.14 or a newer version, a protection recommendation appears. This recommendation appears because we need permissions to scan your entire system for threats. To give us permissions, you have to be logged in as administrator and follow these steps:
>
> 1. Click the **System Preferences** link.
> 2. Click the icon, and then type in your administrator credentials.
> 3. A new window opens. Drag the **BDLDaemon** file to the allowed apps list.

3.2. App Main Window

Bitdefender Antivirus for Mac 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.

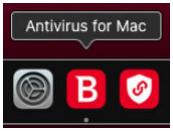
The status bar at the top of the window informs you about the system's security status using explicit messages and suggestive colors. If Bitdefender Antivirus for Mac has no warnings, the status bar is green. When a security issue has been detected, the status bar changes its color into red. For detailed information on issues and how to fix them, refer to Fixing Issues (page 24).

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 or make online payments Bitdefender Autopilot will come up with contextual recommendations based on your device usage and needs. This will help you discovery and benefit from the advantages brought by the features included into the Bitdefender Antivirus for Mac app.

From the navigation menu on the left side you can access the Bitdefender sections for detailed configuration and advanced administrative tasks (**Protection** and **Privacy** tabs), notifications, your Bitdefender account and the Preferences area. Also, you can contact us (**Help** tab) for support in case you have questions or something unexpected appears.

3.3. App Dock Icon

The Bitdefender Antivirus for Mac icon can be noticed in the Dock as soon as you open the app. The icon in the Dock provides you with an easy way to scan files and folders for threats. Just drag and drop the file or folder over the Dock icon and the scan will start immediately.



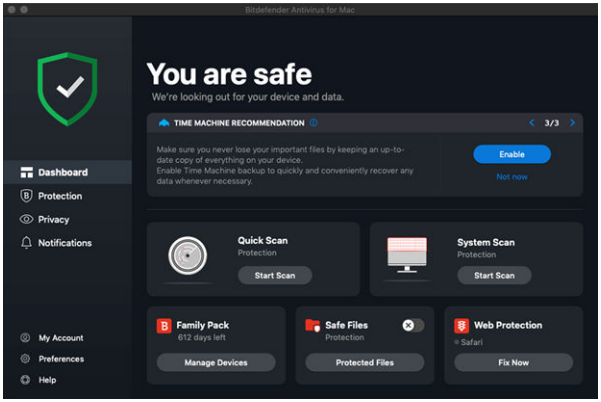
3.4. Navigation Menu

On the left side on the Bitdefender interface is the navigation menu, which enables you to quickly access the Bitdefender features 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, perform quick actions, and go to your Bitdefender account to manage the devices you have added to your Bitdefender subscription.
- **Protection**. From here, you can launch antivirus scans, add files to the exceptions list, protect files and apps from ransomware attacks, secure your Time Machine backups, and configure protection while surfing on the internet.
- **Privacy**. From here, you can open the Bitdefender VPN app and install the Anti-tracker extension in your web browser.
- **Notifications**. From here, you can see details about the actions taken on scanned files.
- **My Account**. From here, you can see the Bitdefender account and subscription by which your device is protected, as well as switch your account if needed.
- **Preferences**. From here, you can configure the Bitdefender settings.
- **Help**. From here, whenever you need assistance in solving a situation with your Bitdefender product, you can contact the Technical Support department. You can also send us your feedback to help us improve the product.

3.5. Dark Mode

To give your eyes protection against glare and lights while working at night or in a lightless operating condition, Bitdefender Antivirus for Mac supports Dark Mode for Mojave 10.14 and later. The colors of the interface have been optimized so that you can use your Mac without straining your eyes. The Bitdefender Antivirus for Mac interface adjusts itself depending on your device appearance seetings.



4. PROTECTING AGAINST MALICIOUS SOFTWARE

This chapter includes the following topics:

4.1. Best Practices

To keep your system protected against threats and to prevent accidental infection of other systems, follow these best practices:

- Keep **Bitdefender Shield** enabled, as to allow system files to be automatically scanned by Bitdefender Antivirus for Mac.
- Maintain your Bitdefender Antivirus for Mac product up to date with the latest threat information and product updates.
- Check and fix the issues reported by Bitdefender Antivirus for Mac regularly. For detailed information, refer to Fixing Issues (page 24).
- Check the detailed log of events concerning the Bitdefender Antivirus for Mac 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. For more details, access Notifications (page 25).

- You should also adhere to these best practices:
  - Make a habit of scanning files that you download from an external storage memory (such as an USB stick or a CD), especially when you do not know the source.
  - If you have a DMG file, mount it and then scan its contents (the files within the mounted volume/image).

  The easiest way to scan a file, a folder or a volume is to drag & drop it over the Bitdefender Antivirus for Mac window or Dock icon.

No other configuration or action is required. However, if you want to, you can adjust the app settings and preferences to better suit your needs. For more information, refer to Configuring Preferences (page 33).

4.2. Scanning Your Mac

Beside the **Bitdefender Shield** feature, which monitors the installed apps on a regular basis, looking for threat-like actions and prevents new threats from entering your system, you can scan your Mac or specific files anytime you want.

The easiest way to scan a file, a folder or a volume is to drag&drop it over the Bitdefender Antivirus for Mac window or Dock icon. The scan wizard will appear and guide you through the scanning process.

You can also start a scan as follows:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. Select the **Antivirus** tab.
3. Click one of the three scan buttons to start the desired scan.
   - **Quick Scan** - checks for threats the most vulnerable locations on your system (for example, the folders that contain the documents, downloads, mail downloads and temporary files of each user).
   - **System Scan** - performs a comprehensive check for threats of the entire system. All connected mounts will be scanned too.

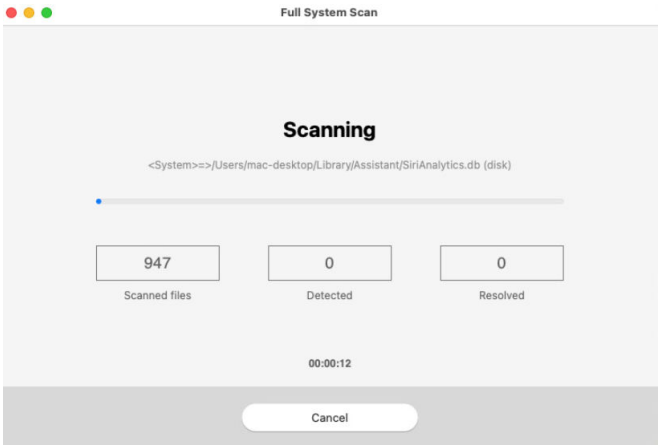
> **Note**
> Depending on the size of your hard disk, scanning the entire system may take a while (up to an hour or even more). For improved performance, it is recommended not to run this task while performing other resource-intensive tasks (such as video editing).
>
> If you prefer, you can choose not to scan specific mounted volumes by adding them to the Exceptions list from the Protection window.

- **Custom Scan** - helps you check specific files, folders or volumes for threats.

You can also start a System or Quick Scan from Dashboard.

4.3. Scan Wizard

Whenever you initiate a scan, the Bitdefender Antivirus for Mac scan wizard will appear.



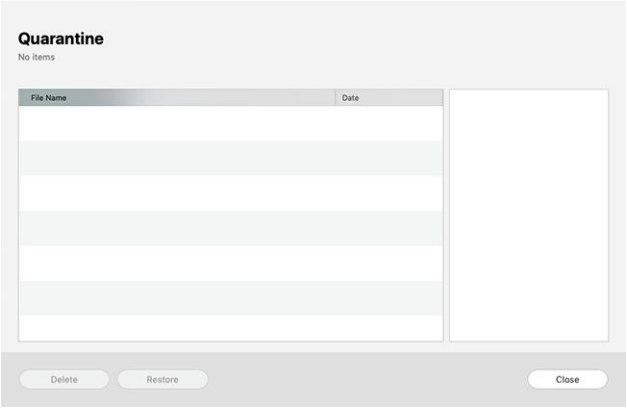
Real-time information about detected and resolved threats is displayed during each Scan.

Wait for Bitdefender Antivirus for Mac to finish scanning.

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

4.4. Quarantine

Bitdefender Antivirus for Mac allows isolating the infected or 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.



The Quarantine section displays all the files currently isolated in the Quarantine folder.

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

To view a list with all the items added to quarantine:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. Click **Open** in the **Quarantine** pane.

4.5. Bitdefender Shield (real-time protection)

Bitdefender provides real-time protection against a wide range of threats by scanning all installed apps, their updated versions, and new and modified files.

To disable the real-time protection:

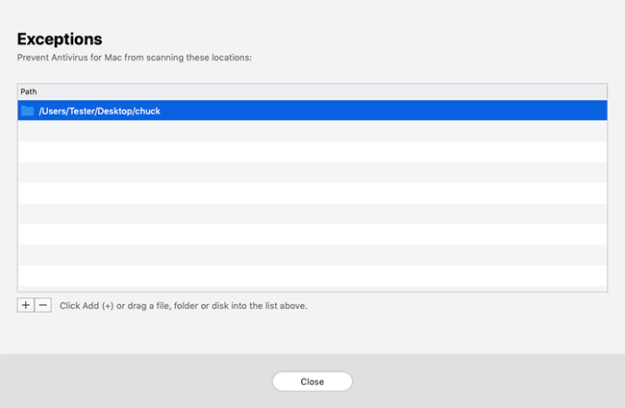
1. Click **Preferences** on the navigation menu on the Bitdefender interface.
2. Turn off **Bitdefender Shield** in the **Protection** window.

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.

4.6. Scan Exceptions

If you want to, you can set Bitdefender Antivirus for Mac not to scan specific files, folders, or even an entire volume. For example, you might want to exclude from scanning:

- Files that are mistakenly identified as infected (known as false positives)
- Files that cause scanning errors
- Backup volumes



The exceptions list contains the paths that have been excepted from scanning.

To access the exceptions list:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. Click **Open** in the **Exceptions** pane.

There are two ways to set a scan exception:

- Drag&drop a file, folder or volume over the exceptions list.

- Click the button labeled with the plus sign (+), located under the exceptions list. Then, choose the file, folder or volume to be excepted from scanning.

To remove a scan exception, select it from the list and click the button labeled with the minus sign (-), located under the exceptions list.

4.7. Web Protection

Bitdefender Antivirus for Mac uses the TrafficLight extensions to completely secure your web browsing experience. The TrafficLight extensions intercept, process and filter all web traffic, blocking malicious content.

The extensions work and integrate with the following web browsers: Mozilla Firefox, Google Chrome and Safari.

4.7.1. Enabling TrafficLight extensions

To enable the TrafficLight extensions:

1. Click **Fix Now** in the **Web protection** card on Dashboard.
2. The **Web protection** window opens.
   The detected web browser you have installed on your system appears. To install the TrafficLight extension on your browser, click **Get Extension**.
3. You are redirected to:
   https://bitdefender.com/solutions/trafficlight.html
4. Select **Free Download**.
5. Follow the steps to install the TrafficLight extension corresponding to your web browser.

4.7.2. Managing extensions settings

An array of features is available to protect you from all kinds of threats you may encounter while web browsing. To access them, click the TrafficLight icon next to your browser's settings, and then click the ⚙ **Settings** button:

- **Bitdefender TrafficLight Settings**
  - Web Protection - prevents you from accessing websites used for malware, phishing and fraud attacks.

- Search Advisor - provides advance warning of risky websites within your search results.

- **Exceptions**
  If you are on the website you want to add to exceptions, click **Add current website to the list**.
  If you would like to add another website, type its address in the corresponding field, and then click .
  No warning will be displayed in case threats are present on the excepted pages. This is why only websites you fully trust should be added to this list.

4.7.3. Page rating and alerts

Depending on how TrafficLight classifies the webpage you are currently viewing, one of the following icons is displayed in its area:

This is a safe page to visit. You can continue your work.

This webpage may contain dangerous content. Exercise caution if you decide to visit it.

You should leave the webpage immediately as it contains malware or other threats.

In Safari, the background of the TrafficLight icons is black.

4.8. Anti-tracker

Many websites you visit are using trackers to collect information about your behavior, either to share it with third-party companies or to show ads that are more relevant for you. Hereby, websites owners are making money to be able to provide you content for free or continue operating. Besides collecting information, trackers can slow down your browsing experience or waste your bandwidth.

With Bitdefender Anti-tracker extension activated in your web browser, you avoid to be tracked so that your data remains private while you browse online and you speed up the time websites need to load.

The Bitdefender extension is compatible with the following web browsers:

- Google Chrome

- Mozilla Firefox
- Safari

The trackers we detect are grouped in the following categories:

- **Advertising** - used to analyze website traffic, user behavior or visitors' traffic patterns.
- **Customer Interaction** - used to measure user interaction with different input forms such as chat or support.
- **Essential** - used to monitor critical webpage functionalities.
- **Site Analytics** - used to gather data regarding webpage usage.
- **Social Media** - used to monitor social audience, activity and user engagement with different social media platforms.

4.8.1. Activating Bitdefender Anti-tracker

To activate the Bitdefender Anti-tracker extension in your web browser:

1. Click **Privacy** on the navigation menu on the Bitdefender interface.
2. Select the **Anti-tracker** tab.
3. Click **Enable extension** next to the web browser for which you want to activate the extension.

4.8.2. Anti-tracker interface

When the Bitdefender Anti-tracker extension is activated, the  icon appears next to the search bar in your web browser. Every time you visit a website, a counter can be noticed on the icon, referring to the detected and blocked trackers. To view more details about the blocked trackers, click the icon to open the interface. Besides the number of the trackers blocked, you can view the time required for the page to load and the categories to which the detected trackers belong. To view the list of the websites that are tracking, click the desired category.

To disable Bitdefender from blocking trackers on the website you are currently visiting, click **Pause protection on this website**. This setting applies only as long you have the website open and will be reverted to the initial state when you close the website.

To allow trackers from a specific category to monitor your activity, click the desired activity, and then click the corresponding button. If you change your mind, click the same button once again.

4.8.3. Turning Bitdefender Anti-tracker off

To turn off the Bitdefender Anti-tracker from your web browser:

1. Open your web browser.
2. Click the icon next to the address bar in your web browser.
3. Click the icon in the upper-right corner.
4. Use the corresponding switch to turn off.
   The Bitdefender icon turns grey.

4.8.4. Allowing a website to be tracked

If you would like to be tracked while you visit a particular website, you can add its address to exceptions as follows:

1. Open your web browser.
2. Click the icon next to the search bar.
3. Click the icon in the upper-right corner.
4. If you are on the website you want to add to exceptions, click **Add current website to the list**.
   If you would like to add another website, type its address in the corresponding field, and then click .

4.9. 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.

Using the latest technology, Bitdefender ensures system integrity by protecting critical system areas against ransomware attacks without impacting the system. However, you may also want to protect your personal files such as documents, photos, or movies from being accessed by untrusted apps. With Bitdefender Safe Files you can settle personal files

to a shelter and configure on your own which apps should be allowed to make changes in the protected files and which should not.

To add afterwards files to the protected environment:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. Select the **Anti-Ransomware** tab.
3. Click **Protected Files** in the Safe Files area.
4. Click the button labeled with the plus sign (+), located under the protected files list. Then, choose the file, folder or volume to be protected in case ransomware attacks will try access them.

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

By default, the folders Pictures, Documents, Desktop, and Downloads are protected against threat attacks.

> **Note**
> Custom folders can be protected only for current users. External drives, system and app files cannot be added to the protection environment.

You will be informed each time an unknown app with an unusual behavior will try to modify the files you added. Click **Allow** or **Block** to add it to the Managing Applications list.

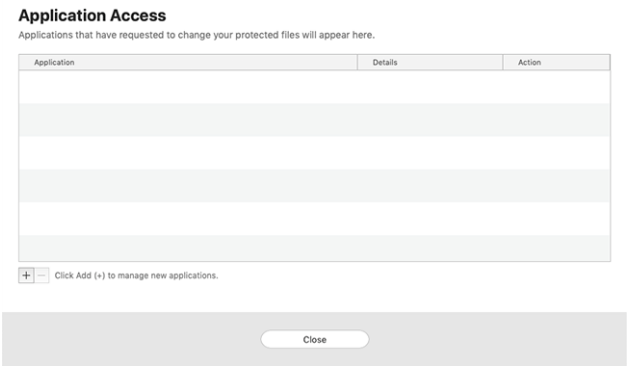
4.9.1. Applications Access

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. Select the **Anti-Ransomware** tab.
3. Click **Application Access** in the Safe Files area.
4. Change the status to Allow next to the blocked app.

Apps that are set on Allow can be set on Blocked as well.

Use the drag&drop method or click the plus sign (+) to add more apps to the list.



4.10. Time Machine Protection

Bitdefender Time Machine Protection serves as an additional layer of security for your backup drive, including all the files you have decided to store in it, by blocking the access of any external source. In case files from your Time Machine drive will be encrypted by ransomware, you will be able to recover them without paying for the asked ransom.

In case you need to restore items from a Time Machine backup, please check the Apple support page for instructions.

4.10.1. Turning on or off Time Machine Protection

To turn on or off disable Time Machine Protection:

1. Click **Protection** on the navigation menu on the **Bitdefender interface**.
2. Select the **Anti-Ransomware** tab.
3. Enable or disable the **Time Machine Protection** switch.

4.11. Fixing Issues

Bitdefender Antivirus for Mac automatically detects and informs you about a series of issues that can affect the security of your system and data. In this way, you can fix security risks easily and in a timely manner.

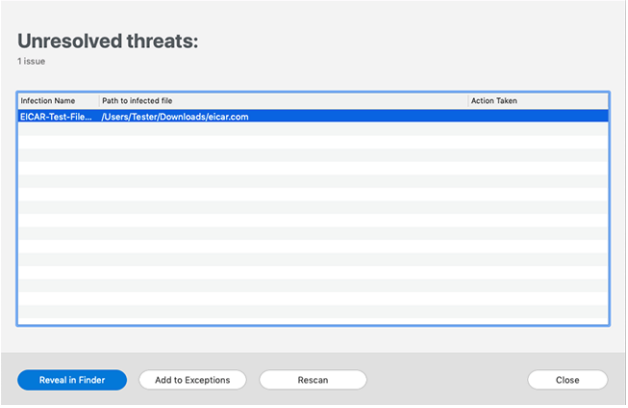
Fixing the issues indicated by Bitdefender Antivirus for Mac is a quick and easy way to ensure optimal protection of your system and data.

Detected issues include:

- The new threat information update was not been downloaded from our servers.
- Threats have been detected on your system and the product cannot automatically disinfect them.
- The real-time protection is disabled.

To check and fix detected issues:

1. If Bitdefender has no warnings, the status bar is green. When a security issue has been detected, the status bar changes its color into red.
2. Check the description for more information.
3. When a issue is detected, click the corresponding button to take action.



The list of unresolved threats is updated after each system scan no matter whether the scan is automatically made in the background or initiated by you.

You can choose to take the following actions on unresolved threats:

- Manually delete. Take this action to remove the infections manually.
- Add to Exceptions. This action is not available for threats found inside archives.

4.12. 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.

4.13. Updates

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

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

- If Bitdefender Antivirus for Mac is up-to-date, it can detect the latest threats discovered and clean the infected files.

- If Bitdefender Antivirus for Mac is not up-to-date, it will not be able to detect and remove the latest threats discovered by Bitdefender Labs.

4.13.1. Requesting an Update

You can request an update manually anytime you want.

An active internet connection is required to check for available updates and download them.

To request an update manually:

1. Click the **Actions** button in the menu bar.
2. Choose **Update threat information database**.

Alternatively, you can request an update manually by pressing CMD + U.

You can see the update progress and downloaded files.

4.13.2. Getting Updates through a Proxy Server

Bitdefender Antivirus for Mac can update only through proxy servers that do not require authentication. You do not have to configure any program settings.

If you connect to the internet through a proxy server that requires authentication, you must switch to a direct internet connection regularly to obtain threat information updates.

4.13.3. Upgrade to a new version

Occasionally, we launch product updates to add new features and improvements or fix product issues. These updates may require a system restart to initiate the installation of new files. By default, if an update requires a computer restart, Bitdefender Antivirus for Mac will keep working with the previous files until you reboot the system. In this case, the update process will not interfere with the user's work.

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 to upgrade** from the menu bar or manually restart the system.

4.13.4. Finding information about Bitdefender Antivirus for Mac

To find information about the Bitdefender Antivirus for Mac version you have installed, access the **About** window. In the same window you can access and view the Subscription Agreement, Privacy Policy and Open-source licenses.

To access the About window:

1. Open Bitdefender Antivirus for Mac.
2. Click Bitdefender Antivirus for Mac in the menu bar and choose **About Antivirus for Mac**.

5. VPN

This chapter includes the following topics:

5.1. About VPN

With Bitdefender VPN you can keep your data private each time you connect to unsecured wireless networks while in airports, malls, cafés, or hotels. This way, unfortunate situations such as theft of personal data, or attempts to make your device's IP address accessible to hackers can be avoided.

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 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.

5.2. Opening VPN

There are three ways to open the Bitdefender VPN app:

- Click **Privacy** on the navigation menu on the **Bitdefender interface**. Click **Open** in the Bitdefender VPN card.
- Click the icon from menu bar.
- Go to the Applications folder, open the Bitdefender folder, and then double-click the Bitdefender VPN icon.

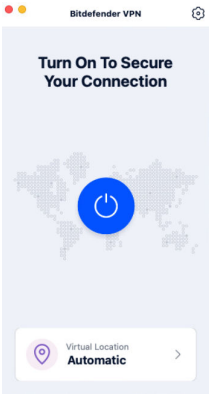
The first time you open the app, you are requested to allow Bitdefender to add configurations. By allowing Bitdefender to add configurations, you agree that all network activity of your device can be filtered or monitored when using the VPN app.

> **Note**
> The Bitdefender VPN app can only be installed on macOS Sierra (10.12.6), macOS High Sierra (10.13.6), or macOS Mojave (10.14) or later versions of the operating system.

5.3. 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 by selecting it from the Virtual Locations list. For details about VPN subscriptions, refer to Subscriptions (page 32).

To connect or disconnect, simply click on the status displayed at the top of the screen. The menu bar icon shows black when the VPN is connected, and white when the VPN is disconnected.



While connected, the elapsed time is displayed on the lower part of the interface. To get access to more options, click the icon in the upper-right side:

- **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:
  - **General**
    - Notifications - Display product notifications.
    - Run at Startup - Automatically launch Bitdefender VPN at Login.
    - Product reports - Submit anonymous product reports to help us improve your experience and protection capabilities.
  - **Advanced**
    - Internet Kill-Switch - Temporarily suspends all internet traffic if the VPN connection accidentally drops.
    - Ad blocker and Anti-tracker - Block ads and trackers in order to enjoy a cleaner and faster web.
    - Split tunneling - Selected websites will bypass the VPN and access the Internet directly.

      Note
      Click **Manage** and then **Add website** in order to add webpages to this list.

    - Autoconnect - Connect the VPN automatically when:
      - Connecting to an unsecure or public Wi-Fi.
      - A peer-to-peer file sharing app is started.

- **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.
- **Quit** - exit the app.

5.4. Subscriptions

Bitdefender VPN offers for free a daily 200 MB traffic quota per device to secure the 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 **Upgrade** button available in the product interface.

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

Bitdefender VPN is a cross-platform product, available in the 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.

6. CONFIGURING PREFERENCES

This chapter includes the following topics:

6.1. Accessing Preferences

To open the Bitdefender Antivirus for Mac Preferences window:

- Do any of the following:
  - Click **Preferences** on the navigation menu on the Bitdefender interface.
  - Click Bitdefender Antivirus for Mac in the menu bar and choose **Preferences**.

6.2. Protection Preferences

The protection preferences window allows you to configure the overall scanning approach. You can configure the actions taken on the infected and suspicious files detected and other general settings.

- **Bitdefender Shield.** Bitdefender Shield provides real-time protection against a wide range of threats by scanning all installed apps, their updated versions, and new and modified files. We do not recommend you to disable Bitdefender Shield, but if you have to, do it for as little time as possible. If Bitdefender Shield is disabled, you will not be protected against threats.
- **Scan only new and changed files.** Select this check box to set Bitdefender Antivirus for Mac to scan only files that have not been scanned before or that have been modified since their last scan.

  You can choose not to apply this setting for custom and drag & drop scanning by clearing the corresponding check box.
- **Don't scan content in backups.** Select this check box to exclude backup files from scanning. If the infected files are restored at a later time,

Bitdefender Antivirus for Mac will automatically detect them and take the proper action.

6.3. Advanced Preferences

You can choose an overall action to be taken for all issues and suspected items found during a scanning process.

Action for infected items

- **Try to disinfect or move to quarantine** - If infected files are detected, Bitdefender will try to disinfect them (remove the malicious code) or to move them to quarantine.
- **Take no action** - No action will be taken on the detected files.

Action for suspected items

- **Move files to quarantine** - If suspected files are detected, Bitdefender will move them to quarantine.
- **Take no action** - No action will be taken on the detected files.

6.4. Special Offers

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 **Preferences** on the navigation menu on the Bitdefender interface.
2. Select the **Other** tab.
3. Turn on or off the **My offers** switch.

> **Note**
> The **My offers** option is enabled by default.

7. ABOUT BITDEFENDER CENTRAL

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

To install the Bitdefender Central app on your devices:

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

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

- Download and install Bitdefender on Windows, macOS, iOS and Android operating systems. The products available for download are:
  - Bitdefender Antivirus for Mac
  - The Bitdefender Windows product line
  - 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.

7.1. Accessing Bitdefender Central

There are several ways to access Bitdefender Central. Depending on the task you want to perform, you can use any of the following possibilities:

- From the Bitdefender Antivirus for Mac main interface:
  1. Click the **Go to your account** link at the lower right part of the screen.

- From your web browser:
  1. Open a web browser on any device with internet access.
  2. Go to: https://central.bitdefender.com.
  3. Sign in to your account using your email address and password.
- From your Android or iOS device:
  1. Open the Bitdefender Central app you have installed.

> **Note**
> In this material we have included the options that you can find on the web interface.

7.2. 2-Factor Authentication

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

7.2.1. Enabling 2-Factor Authentication

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

To enable 2-Factor Authentication:

1. Access Bitdefender Central.
2. Click the icon in the upper right side of the screen.
3. Click **Bitdefender Account** in the slide menu.
4. Select the **Password and security** tab.
5. Click **GET STARTED**.
   Choose one of the following methods:
   - **Authenticator App** - use an authenticator app to generate a code each time you want sign in to your Bitdefender account.

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

a. Click **USE AUTHENTICATOR APP** to start.

b. To sign in on an Android or iOS-based device, use your device to scan the QR code.
To sign in on a laptop or computer, you can add manually the displayed code.
Click **CONTINUE**.

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

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

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

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

  c. Click **ACTIVATE**.

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

1. Click **TURN OFF 2-FACTOR AUTHENTICATION**.
2. Check your app or email account and type in the code you have received.
   In case you have choosen to receive the authentication code via email, you have five minutes to check your email account and type in the generated code. If the time expires, you will have to generate a new code by following the same steps.
3. Confirm your choice.

7.3. Adding trusted devices

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

To add devices as trusted devices:

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

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

7.4. My Devices

The **My Devices** area in your Bitdefender account 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.

7.4.1. Adding a new device

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

1. Access Bitdefender Central.
2. Select the **My Devices** panel, and then tap **INSTALL PROTECTION**.
3. Choose one of the two available options:
   - **Protect this device**
     Select this option, and then select the owner of the device. If the device belongs to someone else, tap the corresponding button.
   - **Protect other devices**
     Select this option, and then select the owner of the device. If the device belongs to someone else, tap the corresponding button.
     Tap **SEND DOWNLOAD LINK**. Type an email address in the corresponding field, and tap **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 tap the corresponding download button.

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

7.4.2. Customize your device

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

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

7.4.3. Remote actions

To remotely update Bitdefender on a device:

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

3. Tap 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, tap the desired device card.

Once you tap 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, tap the drop-down arrow in the upper status area to find out more details.
- **Protection.** From this window you can remotely run a Quick or a System Scan on your devices. Tap 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.
- **Optimizer.** Here you can remotely improve a device's performance by rapidly scanning, detecting and cleaning useless files. Tap the **START** button, and then select the areas you want to optimize. Tap again the **START** button to begin the optimization process. Tap **More details** to access a detailed report about the fixed issues.
- **Anti-Theft.** In case of misplacement, theft or loss, with the Anti-Theft feature you can locate your device and take remote actions. Tap **LOCATE** to find out the position of the device. The last known position will be displayed, along with the time and date.
- **Vulnerability.** To check a device for any vulnerabilities such as missing Windows updates, outdated apps, or weak passwords tap 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. Tap **More details** to access a detailed report about the found issues.

7.5. Activity

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

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

- **My Devices**. Here you can view the number of the connected devices along with their protection status. To fix issues remotely on the detected devices, tap **Fix issues**, and then tap **SCAN AND FIX ISSUES**.
  To view details about the detected issues, tap **View issues**.
  Information about detected threats cannot be retrieved from iOS-based devices.
- **Threats blocked**. Here you can view a graph showing an overall statistic including information about the threats blocked in the last 24 hours and seven days. The displayed information is retrieved depending on the malicious behavior detected on accessed files, apps and URLs.
- **Top users with threats blocked**. Here you can view a top with the users were the most threats have been found.
- **Top devices with threats blocked**. Here you can view a top with the devices were the most threats have been found.

7.6. My Subscriptions

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

7.6.1. 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).

7.6.2. Activate subscription

A subscription can be activated during the installation process by using your Bitdefender account. Together with the activation process, the subscription's 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 your Bitdefender subscription.

To activate a subscription using an activation code, follow these steps:

1. Access Bitdefender Central.
2. Select the **My Subscriptions** panel.
3. Tap the **ACTIVATION CODE** button, then type the code in the corresponding field.
4. Tap **ACTIVATE** to continue.

The subscription is now activated.

7.6.3. Renew Subscription

If you disabled the automatic renewal of 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. Tap **RENEW** to continue.

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

7.7. Notifications

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

8. FREQUENTLY ASKED QUESTIONS

How can I try Bitdefender Antivirus for Mac before applying for a subscription?

You are a new Bitdefender customer and would like to try our product before buying it. The trial period is 30 days and you can continue using the installed product only if you buy a Bitdefender subscription. To try Bitdefender Antivirus for Mac, you have to:

1. Create a Bitdefender account by following these steps:
   a. Go to: https://central.bitdefender.com.
   b. Type the required information in the corresponding fields. The data you provide here will remain confidential.
   c. 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.
   d. Click **CREATE ACCOUNT**.

2. Download Bitdefender Antivirus for Mac as follows:
   a. Select the **My Devices** panel, and then click **INSTALL PROTECTION**.
   b. Choose one of the two available options:
      - **Protect this device**
        i. Select this option, and then select the owner of the device. If the device belongs to someone else, click the corresponding button.
        ii. Save the installation file.
      - **Protect other devices**
        i. Select this option, and then select the owner of the device. If the device belongs to someone else, click the corresponding button.
        ii. Click **SEND DOWNLOAD LINK**.
        iii. 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.

iv. 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.

c. Run the Bitdefender product you have downloaded.

I have an activation code. How do I add its validity to my subscription?

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 your Bitdefender subscription.

To activate a subscription using an activation code, follow these steps:

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 extension is now visible in your Bitdefender account, and in your Bitdefender Antivirus for Mac installed product, in the lower-right part of the screen.

The scan log indicates there are still unresolved items. How do I remove them?

The unresolved items in the scan log may be:

- restricted access archives (xar, rar, etc.)
  Solution: Use the **Reveal in Finder** option to find the file and delete it manually. Make sure to empty the Trash.
- restricted access mailboxes (Thunderbird, etc.)
  Solution: Use the app to remove the entry containing the infected file.
- Content in backups
  Solution: Enable the **Don't scan content in backups** option in Protection Preferences or **Add to Exceptions** the detected files.
  If the infected files are restored at a later time, Bitdefender Antivirus for Mac will automatically detect them and take the proper action.

> **Note**
> Restricted access files means files Bitdefender Antivirus for Mac can only open, but it cannot modify them.

Where can I see details about the product activity?

Bitdefender keeps a log of all important actions, status changes and other critical messages related to its activity. To access this information, click **Notifications** on the navigation menu on the Bitdefender interface.

Can I update Bitdefender Antivirus for Mac through a Proxy Server?

Bitdefender Antivirus for Mac can update only through proxy servers that do not require authentication. You do not have to configure any program settings.

If you connect to the internet through a proxy server that requires authentication, you must switch to a direct internet connection regularly to obtain threat information updates.

How do I remove Bitdefender Antivirus for Mac?

To remove Bitdefender Antivirus for Mac, follow these steps:

1. Open a **Finder** window, and then go to the Applications folder.
2. Open the Bitdefender folder, and then double-click BitdefenderUninstaller.
3. Click **Uninstall** and wait for the process to complete.
4. Click **Close** to finish.

> **Important**
> If there is an error, you can contact Bitdefender Customer Care as described in Asking for Help (page 49).

How do I remove the TrafficLight extensions from my web browser?

- To remove the TrafficLight extensions from Mozilla Firefox, follow these steps:
  1. Go to **Tools** and select **Add-ons**.
  2. Select **Extensions** on the left column.
  3. Select the extension and click **Remove**.
  4. Restart the browser for the removal process to complete.

- To remove the TrafficLight extensions from Google Chrome, follow these steps:
  1. At the top right, click **More** ⋮ .
  2. Go to **More tools** and select **Extensions**.
  3. Click the **Remove** 🗑 icon next to the extension you want to remove.
  4. Click **Remove** to confirm the removal process.
- To remove Bitdefender TrafficLight from Safari, follow these steps:
  1. Go to **Preferences** or press **Command-Comma(,)**.
  2. Select **Extensions**.
     A list with the installed extensions appears.
  3. Select the Bitdefender TrafficLight extension, and then click **Uninstall**.
  4. Click **Uninstall** once again to confirm the removal process.

When should I use Bitdefender VPN?

You have to be careful when you access, download, or upload content on the internet. To make sure you stay safe while browsing the web, we recommend you to use Bitdefender VPN when you:

- want to connect to public wireless networks
- want to access content that normally is restricted in specific areas, no matter if you are home or abroad
- want to keep your personal data private (usernames, passwords, credit card information, etc.)
- want to hide your IP address

Will Bitdefender VPN have a negative impact on the battery life of my device?

Bitdefender VPN is designed to protect your personal data, hide your IP address while connected to unsecured wireless networks, and access restricted content in certain countries. To avoid an unnecessary battery consumption of your device, we recommend you to use the VPN only when you need it, and disconnect when offline.

Why am I encountering internet slowdowns while connected with Bitdefender VPN?

Bitdefender VPN is designed to offer you a light experience while surfing the web; however, your internet connectivity or the server distance you connect to may cause the slowdown. In this case, if it is not a must to connect from your location to a faraway hosted server (e.g. from USA to China), we recommend you to allow Bitdefender VPN to automatically connect you to the nearest server, or find a server closer to your current location.

9. GETTING HELP

9.1. 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.

9.2. Online Resources

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

- Bitdefender Support Center:
  https://www.bitdefender.com/consumer/support/
- The Bitdefender Expert Community:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

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

9.2.1. 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 at the following address: https://www.bitdefender.com/consumer/support/.

9.2.2. The Bitdefender Expert Community

The Expert Community is an environment where Bitdefender users, enthusiasts and fans can engage, exchange ideas, support each other and share their knowledge and solutions. It is also a place of ideation and provides valuable feedback to our development teams. The community members are experienced Bitdefender users happy to help other peers on their own time.

Here you will find meaningful conversations with people that use Bitdefender on their devices. The community offers a true connection with our members and makes your voice heard. It is a place where you are encouraged to participate knowing that your opinion and input are respected and cherished. As a valued provider, we strive to offer an unparalleled level of fast, accurate support and we wish to bring our users closer to us. We have designed our community with this purpose in mind.

You can find our Expert Community webpage here:

https://community.bitdefender.com/en/

9.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia has all the info you need about the latest cyber-threats. This is the place where Bitdefender experts share tips & tricks about how to stay protected from hackers, data breaches, identity theft and social impersonation attempts.

The Bitdefender Cyberpedia webpage can be found here:

https://www.bitdefender.com/cyberpedia/.

9.3. 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 directly through our **Bitdefender Support Center:**

https://www.bitdefender.com/consumer/support/

9.3.1. 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.

GLOSSARY

Activation code

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

ActiveX

ActiveX is a model for writing programs so that other programs and the operating system can call them. ActiveX technology is used with Microsoft Internet Explorer to make interactive webpages that look and behave like computer programs, rather than static pages. With ActiveX, users can ask or answer questions, use push buttons, and interact in other ways with the webpage. ActiveX controls are often written using Visual Basic. Active X is notable for a complete lack of security controls; computer security experts discourage its use over the internet.

Advanced persistent threat

Advanced persistent threat (APT) exploits vulnerabilities of systems to steal important information to deliver it to the source. Big groups such as organizations, companies, or governments, are targeted by this threat. The objective of an advanced persistent threat is to remain undetected for a long time being able to monitor and gather important information without damaging the targeted machines. The method used to inject the threat into the network is through a PDF file or an Office document that look harmless so that every user can run the files.

Adware

Adware is often combined with a host app that is provided at no charge as long as the user agrees to accept the adware. Because adware apps are usually installed after the user has agreed to a licensing agreement that states the purpose of the app, no offense is committed. However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these apps collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

Archive

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

A file that contains one or more files in a compressed format.

Backdoor

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

Boot sector

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot sector also contains a program that loads the operating system.

Boot virus

A threat that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the threat to become active in memory. Every time you boot your system from that point on, you will have the threat active in memory.

Botnet

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

Browser

Short for web browser, a software app used to locate and display webpages. Popular browsers include Microsoft Internet Explorer, Mozilla Firefox and Google Chrome. These are graphical browsers, which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.

Brute Force Attack

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

Command line

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

Cookies

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

Cyberbullying

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

Dictionary Attack

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

Disk drive

It's a machine that reads data from and writes data onto a disk. A hard disk drive reads and writes hard disks. A floppy drive accesses floppy disks.

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

Download

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

Email

Electronic mail. A service that sends messages on computers via local or global networks.

Events

An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

Exploits

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

False positive

Occurs when a scanner identifies a file as infected when in fact it is not.

Filename extension

The portion of a filename, following the final point, which indicates the kind of data stored in the file. Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

Heuristic

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

Honeypot

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

IP

Internet Protocol - A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

Java applet

A Java program which is designed to run only on a webpage. To use an applet on a webpage, you would specify the name of the applet and the size (length and width, in pixels) that the applet can utilize. When the webpage is accessed, the browser downloads the applet from a server and runs it on the user's machine (the client). Applets differ from apps in that they are governed by a strict security protocol.

For example, even though applets run on the client, they cannot read or write data onto the client's machine. Additionally, applets are further restricted so that they can only read and write data from the same domain that they are served from.

Keylogger

A keylogger is an app that logs anything you type. Keyloggers are not malicious in nature. They can be used for legitimate purposes, such as monitoring employees or children activity. However, they are increasingly being used by cyber-criminals for malicious purposes (for example, to collect private data, such as login credentials and social security numbers).

Macro virus

A type of computer threat that is encoded as a macro embedded in a document. Many apps, such as Microsoft Word and Excel, support powerful macro languages. These apps allow you to embed a macro in a document, and have the macro execute each time the document is opened.

Mail client

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

Memory

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips, and the word storage is used for memory that exists on tapes or disks. Every computer comes with a certain amount of physical memory, usually referred to as main memory or RAM.

Non-heuristic

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

Online predators

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

Packed programs

A file in a compression format. Many operating systems and apps contain commands that enable you to pack a file so that it takes up less memory. For example, suppose you have a text file containing ten consecutive space characters. Normally, this would require ten bytes of storage.

However, a program that packs files would replace the space characters by a special space-series character followed by the number of spaces being replaced. In this case, the ten spaces would require only two bytes. This is just one packing technique - there are many more.

Path

The exact directions to a file on a computer. These directions are usually described by means of the hierarchical filing system from the top down.

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

Phishing

The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, social security, and

bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the user's information.

Photon

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

Polymorphic virus

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

Port

An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

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

Ransomware

Ransomware is a malicious program that tries to make money from users by locking their vulnerable systems. CryptoLocker, CryptoWall, and TeslaWall, are only some variants that hunt personal systems of users.

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

Report file

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

Rootkit

A rootkit is a set of software tools which offer administrator-level access to a system. The term was first used for the UNIX operating systems and it

referred to recompiled tools which provided intruders administrative rights, allowing them to conceal their presence so as not to be seen by the system administrators.

The main role of rootkits is to hide processes, files, logins and logs. They may also intercept data from terminals, network connections or peripherals, if they incorporate the appropriate software.

Rootkits are not malicious in nature. For example, systems and even some apps hide critical files using rootkits. However, they are mostly used to hide threats or to conceal the presence of an intruder into the system. When combined with threats, rootkits pose a great threat to the integrity and the security of a system. They can monitor traffic, create backdoors into the system, alter files and logs and avoid detection.

Script

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

Spam

Electronic junk mail or junk newsgroup postings. Generally known as any unsolicited email.

Spyware

Any software that covertly gathers user information through the user's internet connection without his or her knowledge, usually for advertising purposes. Spyware apps are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the internet; however, it should be noted that the majority of shareware and freeware apps do not come with spyware. Once installed, the spyware monitors user activity on the internet and transmits that information in the background to someone else. Spyware can also gather information about email addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse threat is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's internet connection. Because spyware is using memory and system

resources, the apps running in the background can lead to system crashes or general system instability.

Startup items

Any files placed in this folder will open when the computer starts. For example, a startup screen, a sound file to be played when the computer first starts, a reminder calendar, or apps can be startup items. Normally, an alias of a file is placed in this folder rather than the file itself.

Subscription

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

System tray

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right-click an icon to view and access the details and controls.

TCP/IP

Transmission Control Protocol/Internet Protocol - A set of networking protocols widely used on the internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

Threat

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

Threat Information Update

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

Trojan

A destructive program that masquerades as a benign app. Unlike malicious software programs and worms, Trojans do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse threats is a program that claims to rid your computer of threats but instead introduces threats onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

Bitdefender has its own update feature that allows you to manually check for updates, or let it automatically update the product.

Virtual Private Network (VPN)

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

Worm

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