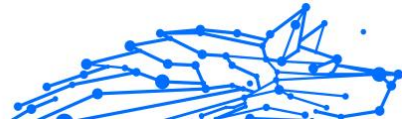# Bitdefender® CONSUMER SOLUTIONS

VPN

Bitdefender VPN

User's Guide

Publication date 31/10/2023
Copyright © 2023 Bitdefender

Legal Notice

Bitdefender®

Table of Contents

ABOUT THIS GUIDE

Purpose and Intended Audience

This guide is intended to all Bitdefender users who have chosen Bitdefender VPN as their go-to service that grants them online anonymity by encrypting all incoming and outgoing traffic on their PC, Mac or mobile devices.

You will find out how to configure and use Bitdefender VPN to keep your online identity and activities safe from hackers, ISPs and snoops. You will learn how to get best from Bitdefender.

We wish you a pleasant and useful lecture.

How to Use This Guide

This guide is organized around several major topics:

What is Bitdefender VPN (page 3)

Get started with Bitdefender VPN by learning what it is and how it can help you protect yourself by granting you true online anonymity.

Using Bitdefender VPN (page 12)

Learn how to interact with Bitdefender VPN and its user interface.

Bitdefender VPN Settings & Features (page 16)

Learn more about the Bitdefender VPN settings and functionalities.

Getting Help (page 29)

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 VPN

The VPN serves as a tunnel between your device and the network you connect to securing your connection, encrypting the data using military-grade encryption, and hiding your IP address wherever you are. Your traffic is redirected through a separate server; thus making your device impossible to be identified by your ISP, 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 feature for the first time. By continuing using the feature, you confirm that you are aware of the applicable country regulations and the risks to which you might be exposed.

1.1. Encryption protocols

The default ciphersuite sets enabled in Hydra client and server are provided below. All other cipher suites are disabled.

Hydra Client ciphersuites:

❍ ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256

❍ ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA

❍ ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA

❍ DHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA:DES-CBC3-SHA

> ⓘ **Note**
> Server side set is much more restrictive and both Hydra client and server will reject a mode different from GCM using AES. Hydra server enforces server side priority of stronger ciphersuites and will reject TLS handshake if weaker suite is requested by a client. This list is also configurable in runtime on the server side.

2. VPN SUBSCRIPTIONS

With Bitdefender VPN, you can opt for two types of subscriptions:

❍ The Basic subscription

❍ The Premium subscription

2.1. Basic subscription

Bitdefender VPN offers for free a daily 200 MB traffic quota per device to secure your connection every time you need and allows you to connect to a single location which cannot be changed.

The Basic subscription is available to any user who downloads Bitdefender VPN.

2.2. Premium subscription

To gain unlimited access to all the features included in Bitdefender VPN, upgrade to the Premium version. Users with an active Premium VPN subscription have unlimited protected traffic and can connect to any of our servers around the world.

There are two plans available for the Premium subscription: the Monthly Plan and the Yearly Plan.

❍ The Monthly Plan: with this plan, you will be charged every month for the Premium VPN services. You can opt-out whenever you wish.

❍ The Yearly Plan: requires a one-time payment, granting you access to our Premium VPN services for an entire year.

2.3. How to upgrade to Premium VPN

The easiest way to upgrade to the Premium version of Bitdefender VPN is to click on the **Upgrade** button situated in the lower part of the main interface. Choose the desired subscription model, then follow the on-screen instructions.

If you already have an activation code, follow the instructions below:

❍ **For Windows users**

1. Click the My Account icon on the left-hand side of the VPN interface.

2. Click **Add it here**.

3. Type in the code received via e-mail, then click the **Activate Code** button.

❍ **For macOS users**

1. Click the cogwheel in the upper-right corner of the VPN interface and select **My Account**.

2. Click **Add it here**.

3. Type in the code received via e-mail, then click the **Activate Code** button.

❍ **For Android users**

1. Tap the cogwheel in the upper-right corner of the VPN interface and select **My Account**.

2. Tap **Add code**.

3. Type in the code received via e-mail, then click the **Activate Code** button.

❍ **For iOS users**

1. Tap the cogwheel in the upper-right corner of the VPN interface and select **My Account**.

2. Tap **Add code**.

3. Type in the code received via e-mail, then click the **Activate Code** button.

3. THE BITDEFENDER CENTRAL ACCOUNT

In order to use Bitdefender VPN, you need an active Bitdefender Central account. Bitdefender Central is the platform where you have access to the product's online features and services.

From this account, you will be able to:

❍ Download and install Bitdefender VPN on Windows, macOS, iOS and Android operating systems.

❍ Manage and renew your Bitdefender subscriptions.

3.1. Accessing Bitdefender Central

To access Bitdefender Central, follow the instructions below:

❍ **For Windows users**

1. Click the My Account icon on the left-hand side of the VPN interface.

2. Click **Edit profile**.

❍ **For macOS users**

1. Click the My Account icon on the left-hand side of the VPN interface.

2. Click **Edit profile**.

❍ **For Android users**

1. Tap the cogwheel in the upper-right corner of the VPN interface and select **My Account**.

2. Tap **Edit Account info in Bitdefender Central**.

❍ **For iOS users**

1. Tap the cogwheel in the upper-right corner of the VPN interface and select **My Account**.

2. 2. Tap **Edit Account info in Bitdefender Central**.

Alternatively, you can go to your Bitdefender Central account by accessing https://central.bitdefender.com.

4. INSTALLATION

4.1. Preparing for installation

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

❍ Make sure that the device where you plan to install Bitdefender meets the system requirements. If the device does not meet all the system requirements, Bitdefender will not be installed or, if installed, it will not work properly and it will cause system slowdowns and instability.
For the complete list of all system requirements, refer to System requirements (page 7)

❍ Log on to the device using an Administrator account.

❍ It is recommended that your device be connected to the internet during the installation, even when from a CD/DVD. If newer versions of the app files included in the installation package are available, Bitdefender can download and install them.

4.2. System requirements

❍ **For Windows users**

   ❍ **Operating System:** Windows 7 with Service Pack 1, Windows 8, Windows 8.1, Windows 10 and Windows 11

   ❍ **Memory (RAM):** 1 GB

   ❍ **Available free hard disk space:** 500 MB free space

   ❍ **Net Framework:** min version 4.5.2

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

❍ **For macOS users**

   ❍ **Operating System:** macOS Sierra (10.12) or later

   ❍ **Available free hard disk space:** 100MB free space

❍ **For Android users**

  ❍ **Operating System:** Android 5.0 or later

  ❍ **Storage:** 100MB

  ❍ An active Internet connection

❍ **For iOS users**

  ❍ **Operating System:** iOS 12 or later

  ❍ **Storage on iPhone:** 50MB

  ❍ **Storage on iPad:** 100MB

  ❍ An active Internet connection

4.3. Installing Bitdefender VPN

To begin the installation, follow the instructions corresponding to the operating system you use:

❍ **For Windows users**

1. To begin the installation of Bitdefender VPN on a Windows PC, simply start by downloading the installation kit from https://www.bitdefender.com/solutions/vpn/download or from the e-mail received after a purchase.

2. Double-click the downloaded installer to run it.

3. Choose Yes if presented with the User Account Control dialog box.

4. Wait until the download completes.

5. Select the product language using the drop-down menu on the installer.

6. Check the box "I confirm that I have read and I agree with the Subscription Agreement and Privacy Policy", then click **START INSTALLATION**.

7. Wait until the installation completes.

8. **SIGN IN** with your Bitdefender Central account. If you don't have a Central account, sign up for one by clicking the button **CREATE ACCOUNT**.

9. Choose **I have an Activation Code** if you've purchased a Premium VPN subscription.
Otherwise, you can choose **START TRIAL** to test out the product for free for 7 days before committing to paying for it.

10. Type in the code received via e-mail, then click the **ACTIVATE PREMIUM** button.

11. After a short wait, Bitdefender VPN is installed and ready to be used on your computer.

❍ **For macOS users**

1. To begin the installation of Bitdefender VPN on macOS, simply start by downloading the installation kit from https://www.bitdefender.com/solutions/vpn/download or from the e-mail received after a purchase.

2. The installer will be saved on the Mac. In the Downloads folder, double-click the package file.

3. Follow the on-screen instructions. Choose **Continue**.

4. You will be guided through the steps necessary to install Bitdefender VPN on your Mac. Click twice the **Continue** button.

5. Click **Agree**, after you read and agree to the terms of the software license agreement.

6. Click **Install**.

7. Enter an administrator username and password, then click **Install Software**.

8. You will be notified that a system extension signed by Bitdefender has been blocked. This is not an error, only a security check. Click **Open Security Preferences**.

9. Click the lock icon to unlock it.
Enter an administrator name and password, then press **Unlock**.

10. Click **Allow** to load Bitdefender's system extension. Then close the Security and Privacy window and the installer.

11. Access the shield icon on the menu bar, then **Sign In** with your Bitdefender Central account. If you don't have a Central account, please sign up for one.

12. Choose I have an **Activation Code** if you've purchased a Premium VPN subscription.
Otherwise, you can choose **START TRIAL** to test out the product for free for 7 days before committing to paying for it.

13. Type in the code received via e-mail, then click the **Activate Code** button.

14. After a short wait, Bitdefender VPN is installed and ready to be used on your Mac.

❍ **For Android users**

1. To install Bitdefender VPN on Android, first open the **Google Play Store** app on your smartphone or tablet.

2. Search for Bitdefender VPN and select this app.

3. Tap the **Install** button and wait until the download completes.

4. Tap **Open** to run the app.

5. Check the box "I agree with the Subscription Agreement and Privacy Policy", then tap **Continue**.

6. **Sign In** with your Bitdefender Central account. If you don't have a Central account, sign up for one by tapping **Create Account**.

7. Choose **I have an activation code** if you've purchased a Premium VPN subscription.
Otherwise, you can choose Start 7 days Trial to test out the product for free for 7 days before committing to paying for it.

8. Type in the code received via e-mail, then tap **Activate code**.

❍ **For iOS users**

1. To install Bitdefender VPN on iOS, first open **App Store** on your iPhone or iPad.

2. Search for Bitdefender VPN and select this app.

3. Tap the **Get** icon and wait until the download completes.

4. Tap **Open** to run the app.

5. Check the box **I agree with the Subscription Agreement and Privacy Policy**, then tap **Continue**.

6. **Sign In** with your Bitdefender Central account. If you don't have an account, sign up for one by tapping **Create Account**.

7. Tap **Allow** if you wish to receive Bitdefender VPN notifications.

8. Choose **I have an activation code** if you've purchased a Premium VPN subscription.
    Otherwise, you can choose Start 7 days Trial to test out the product for free for 7 days before committing to paying for it.

9. Type in the code received via e-mail, then tap **Activate code**.

5. USING BITDEFENDER VPN

5.1. Opening Bitdefender VPN

❍ **For Windows**

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

❍ **From the system tray**

Right-click the red shield icon in the system tray, and then select **Show** in the menu.

❍ **From the Bitdefender interface**

If a Bitdefender security product such as Bitdefender Total Security or Bitdefender Antivirus Plus etc. is already installed on your Windows computer, you can open Bitdefender VPN from there:

1. Click **Privacy** on the left sidebar of the Bitdefender interface.

2. Click **Open VPN** on the VPN pane.

❍ **From your desktop**

Double-click the Bitdefender VPN shortcut on your Desktop.

❍ **For macOS**

You can open the Bitdefender VPN app by clicking the ⊘ icon from the menu bar at the top right of the screen.

If the Bitdefender shield cannot be found in the menu bar, use your Mac Launchpad or Finder to bring it back:

❍ **From Launchpad**

1. Press **F4** on your keyboard to enter the Launchpad on your Mac.

2. Browse through the pages of installed apps until you locate the Bitdefender VPN app. Alternatively, you can type **Bitdefender VPN** in Launchpad to start filtering your results.

3. Once you see the Bitdefender VPN app, click on its icon to pin it to the menu bar.

❍ **From Finder**

1. Click on **Finder** at the bottom left of the Dock (Finder is the icon that looks like a blue square with a smiley face).

2. Next, click **Go** at the top left of the screen, on the menu bar.

3. Select **Applications** from the menu to enter the Applications folder on your Mac.

4. From the Applications folder open the **Bitdefender** folder and then double-click the **Bitdefender VPN** app.

> **ⓘ Note**
> In order to access Bitdefender VPN on your Android or iOS mobile devices, simply open the Bitdefender VPN application after you have installed it.

5.2. How to connect to Bitdefender VPN

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 Location list. To connect or disconnect, simply click the power button from the VPN interface.
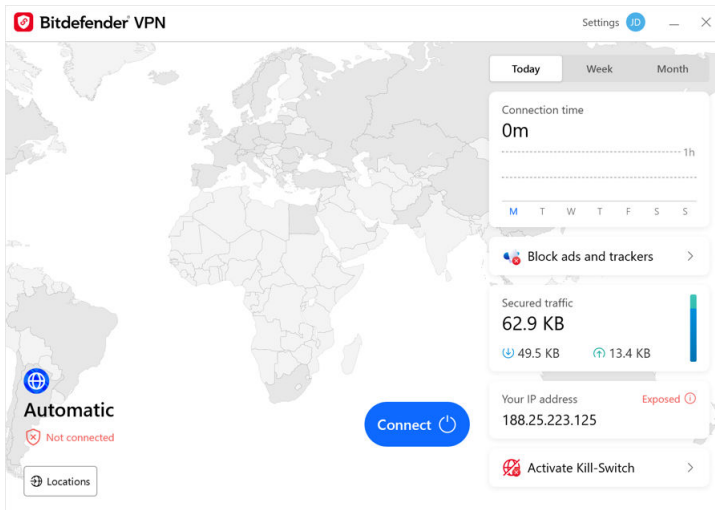
❍ **For Windows:** The system tray icon displays a green checkmark when the VPN is connected, and a black mark when the VPN is disconnected. While connected to a manually selected location, the IP address is displayed on the main interface.

❍ **For macOS:** The menu bar icon 🛡 shows black when the VPN is connected, and 🛡 white when the VPN is disconnected. Click the circular button in the middle of the interface and wait for the connection to be established.

❍ **For Android & iOS:** To connect to Bitdefender VPN for Android, iOS and iPadOS:

  ❍ **In the Bitdefender VPN app:** To connect or disconnect simply tap the power button on the VPN interface. The status of Bitdefender VPN is displayed.

  ❍ **In the Bitdefender Mobile Security app:**

  1. Access the 🛡 VPN icon on the bottom navigation bar of Bitdefender Mobile Security.

  2. Tap **CONNECT** each time you want to stay protected while connected to unsecured wireless networks. Tap **DISCONNECT** whenever you want to disable the VPN connection.

5.3. How to connect to a different server

With a Premium subscription, Bitdefender VPN allows you to connect to any of our servers around the world, at any time. To do this, you will have to:

1. Open the Bitdefender VPN app.

2. Tap the **Locations** button in the lower left corner of the interface.

3. Select any country you wish.

4. Click on the **Connect to [country of choice]** button in the lower part of the interface.

❍ The system tray icon displays a green checkmark when the VPN is connected.

❍ The virtual server's IP address is shown on the home screen while connected to Bitdefender VPN.

❍ A summary of your connection time, the amount of secured traffic, and the last 5 locations you connected to are also shown on the main dashboard.

6. BITDEFENDER VPN SETTINGS & FEATURES

6.1. Accessing Settings

To access the Bitdefender VPN settings, you will have to follow the steps described below:

❍ **On Windows**

1. Open the Bitdefender VPN app on your device by double clicking its icon in the system tray or by right-clicking on it and selecting Show.

2. Click on the **Settings** button (represented by a cogwheel) on the right side of the interface.

❍ **On macOS**

1. Open the Bitdefender VPN app on your macOS device by clicking its icon in the menu bar.

2. Click on the cogwheel button in the upper-right corner of the Bitdefender VPN interface and select Settings.

❍ **On Android**

1. Open the Bitdefender VPN app on your device.

2. Tap on your account in the upper-right corner of the Bitdefender VPN interface.

❍ **On iOS**

1. Open the Bitdefender VPN app on your device.

2. Tap on your account in the upper-right corner of the Bitdefender VPN interface.

6.2. General

Here you can modify the following:

❍ **Open on Startup** – Bitdefender VPN will launch automatically on device startup.

❍ **Show latest locations** – Display the most recent locations on the home screen, for quick access.

❍ **Show dashboard data** – Show trends, stats, and other helpful information on the VPN home screen.

❍ **Clear dashboard data** – All your dashboard data will be erased and all counters reset.

❍ **Theme** – Light/dark theme

❍ **Language** – Change the language of Bitdefender VPN.

❍ **Notifications** – Manage your notifications preferences.

❍ **Help improve Bitdefender VPN** – Submit anonymous product reports to help us improve your experience.

❍ **Reset all settings** – Reset the VPN to its original settings without reinstalling it.
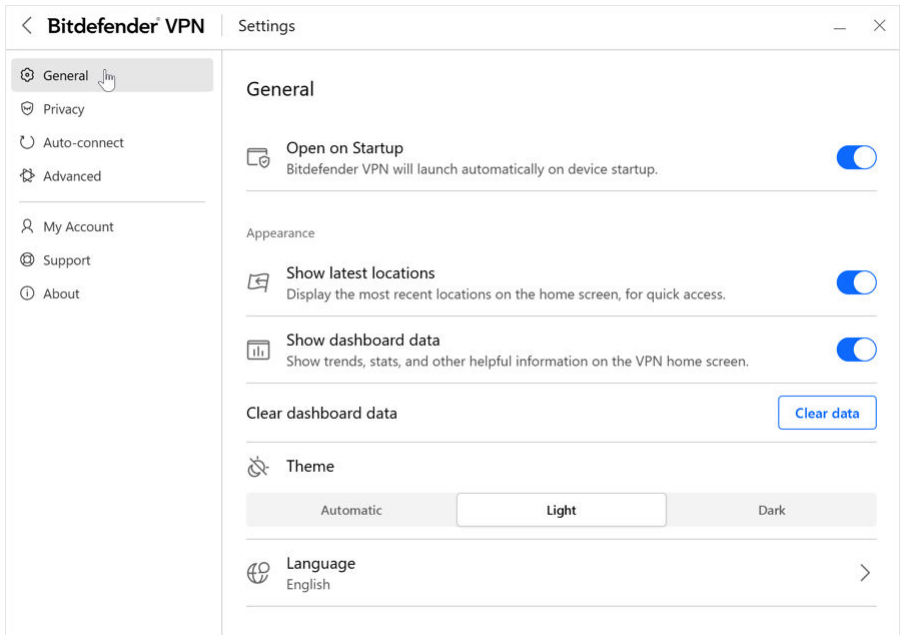
6.3. Features

6.3.1. Privacy

Internet Kill-Switch

The Kill-Switch is a feature implemented in Bitdefender VPN. When enabled, this features temporarily suspends all Internet traffic if the VPN connection accidentally drops. As soon as you are back online, the VPN connection will be reestablished.

To activate the Kill-Switch, follow the steps below:

❍ **On Windows** & **macOS**

1. Open the Bitdefender VPN app on your device by double clicking its icon in the system try or by right-clicking on it and selecting **Show**.

2. Click on the account button on the upper-right side of the interface.

3. Select **Privacy**.

4. Enable the **Internet Kill-Switch** option.

❍ **On Android**

1. Open the Bitdefender VPN app on your device.

2. Click on the account button in the upper-right corner of the Bitdefender VPN interface.

3. Under **Privacy**, enable the **Kill-Switch** option.

❍ **On iOS**

1. Open the Bitdefender VPN app on your device.

2. Click on the account button in the upper-right corner of the Bitdefender VPN interface.

3. Under **Privacy**, enable the **Kill-Switch** option.

> **i** Note
> This feature is also available for macOS devices with operating systems 10.15.4 or later versions.

Ad blocker and Anti-tracker

These features are designed to assist you in staying private and enjoying the web without annoying ads or companies peeking in on you. They help in blocking ads and stopping online trackers.

Ad blocker

The **Ad blocker** is used to block ads, popups, loud video ads or ad banners while browsing. This helps websites load faster and be cleaner, as well as safer to interact with.

To enable the Ad blocker:

1. Locate the **Ad blocker and Antitracker** feature in **Settings - Privacy** .
2. Toggle the switch to the **ON** position.

Anti-tracker

The **Anti-tracker** is used to block trackers set by advertisers to follow and profile you online. Some websites may malfunction when blocking trackers, but adding the URL to the Whitelist may fix this.

To enable the Anti-tracker:

1. Locate the **Ad blocker and Antitracker** feature in **Settings - Privacy**.
2. Toggle the switch to the **ON** position.

Whitelist

Some websites might not load properly if you block their tracker code and ads. Adding the URLs of these specific domains to the whitelist can fix this issue, but keep in mind that, while browsing on these websites, you will see ads and their tracker code will be active.

Add websites you want to allow showing ads and using trackers by:

1. Locate the **Ad blocker and Antitracker** feature in **Settings - Privacy**.
2. Click on the **Manage** link. Then, go to the Whitelist section of the window and click on its corresponding **Manage** link.
3. Click on **Add website** and insert the desired URL.

6.3.2. Auto-connect

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.

To safeguard you against the perils of unsecured or unencrypted public wireless hotspots, Bitdefender VPN includes an auto-connect feature. This means that Bitdefender VPN can be automatically be activated in certain situations, depending on your preferences and the operating system you are running.

❍ On **Windows** the auto-connect feature can be enabled for the following situations:

  ❍ **Startup:** Connect the VPN at Windows startup.

  ❍ **Unsecured Wi-Fi:** Use the VPN whenever you connect to public or unsecured Wi-Fi networks.

  ❍ **Peer-to-peer apps:** Connect to the VPN when you start a peer-to-peer file sharing app.

  ❍ **Apps and domains:** Always use the VPN for certain apps and websites.

  > (i) Note
  > 1. Click the **Manage** link.
  >
  > 2. Browse to the location of the app for which you want to use VPN, select the app name, then click **Add**.

  ❍ **Website categories:** Connect to the VPN when visiting specific website categories. Bitdefender VPN can connect automatically for the following website categories:

    ❍ Financial

    ❍ Online Payments

    ❍ Health

    ❍ File sharing

    ❍ Online Dating

    ❍ Adult Content

> ⓘ **Note**
> For each category, you can select a different server for the VPN to connect to.

❍ On **macOS** the auto-connect feature can be enabled for the following situations:

  ❍ **Startup:** Connect the VPN at macOS startup.

  ❍ **Unsecured Wi-Fi:** Use the VPN whenever you connect to public or unsecured Wi-Fi networks.

  ❍ **Peer-to-peer apps:** Connect to the VPN when you start a peer-to-peer file sharing app.

  ❍ **Applications:** Always connect the VPN for certain apps.

❍ On **Android** and **iOS** Bitdefender VPN can be set to connect automatically only when you're on an unsecured or public Wi-Fi.

6.3.3. Advanced

Split tunneling

Virtual private network (VPN) split tunneling lets you route some of your application or device traffic through an encrypted VPN, while other applications or devices have direct access to the internet. This is particularly useful if you want to benefit from services that perform best when your location is known while also enjoying secure access to potentially sensitive communications and data.

By enabling the **Split tunneling** feature, selected apps and websites will bypass the VPN and access the Internet directly.

To manage the applications and websites that bypass the VPN:

1. Click the **Manage** link once the feature is enabled.

2. Click the **Add** button.

3. Browse to the location of the app in question or insert the URL of the website desired, then click **Add**.

> **Note**
> (i) By adding a website, the entire domain including all subdomains will be bypassed.

> **Important**
> (!) On **macOS** devices, the Split tunneling feature is available only for websites.

App Traffic Optimizer

Bitdefender VPN's App Traffic Optimizer lets you prioritize traffic to the most important apps on your device without exposing your connection to privacy hazards. VPNs redirect Internet traffic through a secure tunnel while using robust encryption algorithms to protect it.

However, this combination of techniques can have some drawbacks, mainly concerning the connection's speed. Several factors can trigger connection slowdowns, the most common being the distance to the server you're connecting to, network congestion, and high bandwidth usage. If you ever felt that sometimes Bitdefender VPN places an unnecessary burden on your connection and slowdowns constantly get in your way, there might be a better answer than disconnecting.

How does App Traffic Optimizer work?

Certain apps and services such as streaming platforms, torrent clients, and games require more bandwidth. Constantly using them could affect your Internet connection speed. Routing your traffic through a VPN tunnel already subjects your connection to a relative slowdown. Placing additional strain on your connection can seriously degrade your online experience.

Bitdefender VPN's App Traffic Optimizer feature can help you tackle VPN connection slowdowns by prioritizing it to the app of your choice. The feature lets you decide what apps should receive the bulk of your traffic, then allocates the resources accordingly. For instance, if you're in a meeting and notice that the quality of your call is subpar, App Traffic Optimizer lets you prioritize traffic to the video conferencing app for improved results.

Typically, VPN users would resort to closing all interfering processes on their device or even disabling their VPN connection to get faster

Internet speed. App Traffic Optimizer lets you enjoy uninterrupted privacy protection without compromising your connection speed.

Using App Traffic Optimizer

Currently, the feature is only available on Windows devices and lets you prioritize traffic to up to 3 applications.

Follow these steps to enable and configure it with minimal effort:

1. Launch the Bitdefender VPN 🔴 application on your Windows computer.
2. Click the account button in the upper-right corner to access the VPN's settings.
3. Head to the **Advanced** tab and enable the **App Traffic Optimizer** feature. The color of the switch will change from gray to blue.

To manage the applications prioritized by this feature:

1. Click the **Manage** link.
2. Browse to the location of the app for which you want to optimize traffic, select the app name, then click **Add**. The app will appear in the **Prioritized** section.

> **ⓘ Note**
> Alternatively, if you have recently opened the application you want to prioritize, press the + button in the App Traffic Optimizer window.

3. Disconnect and reconnect to Bitdefender VPN after adding or removing apps from the list.

To remove an app from App Traffic Optimizer, simply click the 🗑 icon next to the app name.

> **ⓘ Note**
> The App Traffic Optimizer is not available on macOS.

Protocol

Here you can choose the type of protocol you want to use for data transfer. The following options are available:

❍ **Automatic** - Bitdefender VPN will select the optimal protocol for your specific device and network.

❍ **Hydra Catapult** - Fast and secure, ideal for streaming and gaming.

❍ **OpenVPN UDP** - Optimized for fast speeds. However, this protocol is not as reliable in terms of data loss as other protocols in the list.

❍ **OpenVPN TCP** - Designed for reliability. Ensures your data is delivered entirely, but it is not as fast as OpenVPN UDP.

❍ **Wireguard** - Newer protocol, providing strong security and a high level of performance.

Double-hop

With this feature you can manage the servers through which to send and double-encrypt your internet traffic. Your data will pass through two VPN servers instead of one, making it harder to track your internet activity.

> **i** Note
> You can only add a total of 5 double-hop locations. However, you can delete the custom double-hops in your list and create others at any time.

> **!** Important
> Using servers located on different continents in the same double-hop may slow down your connection speed.

7. UNINSTALLING BITDEFENDER VPN

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

❍ **Uninstalling Bitdefender VPN from Windows devices**

  ❍ 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** and **Windows 11**:

    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.

❍ **Uninstalling from macOS devices**

  1. Click on **Go** in the menu bar and select **Applications**.

  2. Double-click on the **Bitdefender** folder.

  3. Run **BitdefenderUninstaller**.

4. In the new window, check the box next to **Bitdefender VPN**, then click on **Uninstall**.

5. Type a valid administrator account name and a password, then click **OK**.

6. Finally, you will be notified that Bitdefender VPN has been successfully uninstalled. Click **Close**.

❍ **Uninstalling from Android devices**

1. Open the **Play Store** app.

2. Search for **Bitdefender VPN**.

3. In the Bitdefender VPN app store page, select **Uninstall**.

4. Confirm by tapping **OK**.

❍ **Uninstalling from iOS devices**

1. Hold your finger on the Bitdefender VPN app.

2. Select **Delete App**.

3. Tap **Delete**.

8. FREQUENTLY ASKED QUESTIONS

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 the VPN when you:

❍ want to connect to public wireless networks

❍ want to access content that is normally restricted in specific areas, no matter if you are home or abroad

❍ want to keep your personal data private (usernames, passwords, email addresses, credit card information, etc.)

❍ want to hide your IP address

Can I choose a city with Bitdefender VPN?

Yes. Currently, Bitdefender VPN for Windows, macOS, Android, and iOS can be used to select a specific city. Here's the list of currently available cities:

❍ **USA:** Atlanta, Charlotte, Chicago, Dallas, Denver, Houston, Los Angeles, Miami, New York, Newark, Phoenix, Portland, San Jose, Seattle, Washington

❍ **Canada:** Montreal, Toronto, Vancouver

❍ **UK:** London, Manchester

Can Bitdefender VPN be installed as a stand-alone app?

The VPN app is installed automatically alongside your Bitdefender security solution. It can also be installed as a standalone app from the product page, from Google Play Store & App Store.

Will Bitdefender share my IP address and personal data shared with third parties?

No, with Bitdefender VPN your privacy is 100% safe. Nobody (advertising agencies, ISPs, insurance companies, etc.) will have access to your online logs.

What encryption algorithm does it use?

Bitdefender VPN uses the Hydra protocol on all platforms, 256-bit AES encryption or the highest available cypher supported by both client and

server, with Perfect Forward Secrecy. This means that encryption keys are generated for each new VPN session and erased from memory when the session is over.

Can I have access to GEO-IP restricted content?

With Premium VPN you have access to an extensive network of virtual locations all over the world.

Will it 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 unnecessary battery consumption of your device, we recommend you to use the VPN only when you need it and disconnect when offline.

Why does the VPN slow down my Internet connection?

Bitdefender VPN is designed to offer a light experience while surfing the web. Depending on the distance between your actual location and the server location you choose to connect to, some speed penalty is expected, however it's almost always sufficiently small that it goes unnoticed during normal online activity. Moreover, we rely on one of the fastest VPN infrastructures in the world. If it is not a must to connect from your location to a faraway hosted server (e.g. from the USA to France), we recommend you allow the 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.