Bitdefender® CONSUMER SOLUTIONS

Ultimate Small Business Security

Bitdefender Ultimate Small Business Security

User's Guide

Publication date 05/31/2024
Copyright © 2024 Bitdefender

Legal Notice

Bitdefender®

Table of Contents

ABOUT THIS GUIDE

Purpose and Intended Audience

Bitdefender Ultimate Small Business Security is a multi-subscription subscription package tailored to meet the cybersecurity needs of small businesses. With a comprehensive feature set, dedicated onboarding, and intuitive management tools, small business owners can protect their digital assets without IT or cybersecurity expertise.

The plan offers comprehensive protection specially designed for small companies, including:

❍ **Multi-platform device protection:** Safeguard all your devices, from computers to mobile phones and servers.

❍ **Easy management:** Maintain the safety of your team and business operations effortlessly.

❍ **Protection for business assets and reputation:** Ensure the highest level of protection for your business by preventing association with fraudulent activities.

❍ **Streamlined Setup:** The onboarding process simplifies setup for non-technical users, ensuring a smooth and secure configuration.

How to Use This Guide

This guide is organized around the products included in Bitdefender Ultimate Small Business Security:

❍ Total Security for Windows PCs & Servers (page 9)
Learn how to use the product on your Windows-based PCs and laptops.

❍ Antivirus for Mac (page 142)
Learn how to use the product on your Macs.

❍ Mobile Security for Android (page 174)
Learn how to use the product on your Android-based smartphones and tablets.

❍ Mobile Security for iOS (page 205)

Learn how to use the product on your iOS-based smartphones and tablets.

❍ VPN (page 219)
Learn how to hide your online identity using Bitdefender VPN on any of your devices.

❍ Password Manager (page 240)
Keep track and safely store of all of your passwords and credentials with Password Manager.

❍ Digital Identity Protection (page 263)
Learn how to properly manage the protection of your digital identity.

❍ Getting Help (page 270)
Find out where to look for help if something unexpected pops up.

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. SETTING UP YOUR SUBSCRIPTION

The process of getting started with your **Bitdefender Ultimate Small Business Security** subscription is specifically tailored to be quick and easy, without the need of IT or cybersecurity expertise. You will need to:

1. **Activate Bitdefender Ultimate Small Business Security:**
   You can do so by following the instructions in the confirmation email received upon purchasing the product.

2. **Set up your business account:**
   Upon activation, you will be asked to enter your business name. This is simply for identification purposes and will be displayed in various places throughout the interface. Note that you can use any name you prefer, as no validation is required for this.

3. **Choose your role in the organization:**

   ❍ **Business Owner:** If you are the business owner and are handling the purchases and setup, select this option.

   ❍ **Security Administrator:** If you are responsible for security administration within the company, choose this option.

   > ⓘ Note
   > The Security Administrator has similar permissions to the business owner, with the exception of purchasing capabilities.

4. **Invite team members to set up accounts:**
   Once you are done with choosing your name and role, you will see an overview of your Bitdefender subscription. From here, you can choose to share the plan with other team members or proceed with your own setup, by following the installation procedures appropriate for the device on which you are looking to install Bitdefender, each outlined in their corresponding chapter within this document.

   > ⚠ Important
   > It is recommended to start by inviting your employees before heading into the installation procedures.

5. **Select team member roles:**

Select the roles of the employees you are inviting to join your business security plan. You can invite them as:

❍ **Security Admin:** This role involves managing members, devices, and security operations, and is intended for those among the employees that have a certain level of understanding in IT, tasked with dealing and monitoring the cybersecurity aspects of your business.

❍ **Employee:** Employees have limited visibility and management capabilities. They will be required a Bitdefender Central account in order to protect their own devices, while those with the **Security Admin** role can oversee their protection and manage their devices remotely.

6. **Send e-mail invitations to team members:**

Type the employees' e-mail addresses you want to share the Bitdefender plan with. Multiple invites can be sent at once.

> (i) Note
>
> Invited members, regardless of role, will receive an email invitation. They must click the **Activate in Bitdefender Central** button and accept the invitation using the same email address they were invited with.

7. **Add sensitive business info to be monitored:**

You will now need to set up business assets exposure monitoring as the final step in the process.

> (i) Note
>
> **Business Assets Exposure** is a service available for administrator roles only. (**Security Admin** and **Business Owner**)

This feature checks for data exposure at the business level in order to protect the company's reputation and prevent any potential targeted attacks.

❍ From the left-hand menu of your Bitdefender Central Account, navigate to the **Business Activity** section.

❍ Click the **Go to setup** button in the **Business Assets Exposure** panel.

❍ Add the requested business information:

  ❍ Business Email

  ❍ Business Credit Card

  ❍ Social Media Accounts

❍ After taking all suggested actions, click the **Mark as done** button to confirm the outcome and track your progress.

Once you are done with these steps, you can start setting up **Bitdefender Ultimate Small Business Security** for yourself:

❍ Install on Windows devices: Installation (page 9)

❍ Install on macOS devices: Installing Bitdefender Antivirus for Mac (page 143)

❍ Install on Android mobile devices: Installing Bitdefender Mobile Security (page 174)

❍ Install on iOS mobile devices: Installing Bitdefender Mobile Security for iOS (page 206)

❍ Install Bitdefender VPN on your devices: Installing Bitdefender VPN (page 221)

❍ Set up Password Manager: Installation (page 242)

❍ Configure Digital Identity Protection: Configure Digital Identity Protection (page 264)

The following of this process marks the successful activation and setup of **Bitdefender Ultimate Small Business Security** for your company.

2. BUSINESS ASSETS EXPOSURE

Business Assets Exposure is a Bitdefender Ultimate Small Business Security service managed by administrators (business owner and security admin) that provides visibility regarding the exposure of key business information in data breaches. Business Assets Exposure monitors 3 components to detect data breaches:

❍ Business Email

❍ Business Credit Card

❍ Social Media Accounts

Why Monitoring Business Assets Exposure is Important:

❍ **Reputation Protection:** Prevents damage to your company's reputation by addressing breaches promptly.

❍ **Employee Safety:** Protects employees from phishing and other social engineering attacks by monitoring and managing their exposed data.

❍ **Targeted Attack Prevention:** Limits the potential for targeted attacks by ensuring sensitive information remains secure.

Once you have set up your **Business Assets Exposure** details as part of the **Setting up your subscription (page 4)** process, you can **review results and act on recommendations:**

The system will inform you of any breaches involving these monitored assets, including the breached services and the types of information exposed (e.g., email addresses, usernames, passwords, geographic locations). Specific details are not shown, only the categories of exposed data.

For each monitored component (business email, business credit card, social media accounts), apply the security recommendations provided. Suggested actions may include:

❍ Asking employees to monitor their business emails with Bitdefender Digital Identity Protection.

❍ Changing passwords on breached websites and advising employees to use Bitdefender Password Manager.

❍ Ensuring that employees install Bitdefender security solutions across devices to prevent any cyberattacks.

❍ Advising employees to use Scam Copilot for advice on potential scams and scam prevention practices.

❍ Monitoring transactions and changing the credit card with the help of the bank issuer.

❍ Enabling two-factor authentication on breached social media platforms to prevent unauthorized logins.

> **i** Note
> After taking the suggested actions, you have to click the **Mark as done** button to confirm completion and track your progress.

By following these steps, administrators can easily monitor and protect their company from data exposure risks using the **Business Assets Exposure** service.

3. TOTAL SECURITY FOR WINDOWS PCS & SERVERS

3.1. Installation

3.1.1. Preparing for installation

Before you install Bitdefender Ultimate Small Business Security, complete these preparations to ensure the installation will go smoothly:

❍ Make sure that the device where you plan to install Bitdefender meets the system requirements. If the device does not meet all the system requirements, Bitdefender will not be installed or, if installed, it will not work properly and it will cause system slowdowns and instability. For a complete list of system requirements, refer to System requirements (page 9).

❍ Log on to the device using an Administrator account.

❍ Remove any other similar software from the device. If any is detected during the Bitdefender installation process, you will be notified to uninstall it. Running two security programs simultaneously may affect their operation and cause major problems with the system. Windows Defender will be disabled during the installation.

❍ Disable or remove any firewall program that may be running on the device. Running two firewall programs simultaneously may affect their operation and cause major problems with the system. Windows Firewall will be disabled during the installation.

❍ 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.

3.1.2. System requirements

You may install Bitdefender Ultimate Small Business Security only on devices running the following operating systems:

❍ Windows 7 with Service Pack 1

❍ Windows 8.1

❍ Windows 10

❍ 2,5 GB available free hard disk space (at least 800 MB on the system drive)

❍ 2 GB of memory (RAM)

You may also install and run Bitdefender Ultimate Small Business Security on the following:

❍ Windows Server 2016 (with Desktop Experience):

  ❍ Standard/RTM

  ❍ Essentials

  ❍ Datacenter

❍ Windows Server 2019 (with Desktop Experience):

  ❍ Standard/RTM

  ❍ Essential

  ❍ Datacenter

❍ Windows Server 2022 (with Desktop Experience):

  ❍ Standard/RTM

  ❍ Datacenter

> **!** **Important**
> System performance may be affected on devices that have old generation CPUs.

> **i** **Note**
> To find out the Windows operating system your device is running and hardware information:
>
> ❍ In **Windows 7**, right-click **My Computer** on the desktop, and then select **Properties** from the menu.
>
> ❍ In **Windows 8.1**, locate **This PC** and then right-click its icon. Select **Properties** in the bottom menu. Look in the **System** area to find information about your system type.
>
> ❍ In **Windows 10** / **Windows 11**, type **System** in the search box from the taskbar and click its icon. Look in the **System** area to find information about your system type.

3.1.3. Software requirements

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

❍ Microsoft Edge 40 and higher

❍ Internet Explorer 11

❍ Mozilla Firefox 51 and higher

❍ Google Chrome 34 and higher

❍ Microsoft Outlook 2007 / 2010 / 2013 / 2016

❍ Mozilla Thunderbird 14 and higher

3.1.4. Installing your Bitdefender product

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

If your purchase covers more than one device, repeat the installation process and activate your product with the same account on every device. The account you need to use is the one which contains your Bitdefender active subscription.

Install from Bitdefender Central

From Bitdefender Central you can download the installation kit corresponding to the purchased subscription. Once the installation process is complete, Bitdefender Ultimate Small Business Security is activated.

To download Bitdefender Ultimate Small Business Security from Bitdefender Central:

1. Access Bitdefender Central.

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

3. Choose one of the two available options:

   ❍ **Protect this device**

   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.

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

Validating the installation

Bitdefender first checks your system to validate the installation.

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

If an incompatible security solution or an older version of Bitdefender is detected, you will be prompted to remove it from your system. Please follow the directions to remove the software from your system, thus avoiding problems occurring later on. You may need to reboot your device to complete the removal of detected security solutions.

The Bitdefender Total Security installation package is constantly updated.

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

Once the installation is validated, the setup wizard appears. Follow the steps to install Bitdefender Ultimate Small Business Security.

Step 1 - Bitdefender installation

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

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

Two additional tasks can be performed at this step:

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

❍ Select the language you want to install the product in.

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

Step 2 - Installation in process

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

Step 3 - Installation completed

Your Bitdefender product is successfully installed.

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

Step 4 - Device Analysis

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

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

When the scan is completed, click **Open Bitdefender Interface**.

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

Step 5 - Get started

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

Click **FINISH** to access the Bitdefender Ultimate Small Business Security interface.

Install from installation disc

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

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

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

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

Validating the installation

Bitdefender first checks your system to validate the installation.

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

If an incompatible security solution or an older version of Bitdefender is detected, you will be prompted to remove it from your system. Please follow the directions to remove the software from your system, thus avoiding problems occurring later on. You may need to reboot your device to complete the removal of detected security solutions.

The Bitdefender Total Security installation package is constantly updated.

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

Once the installation is validated, the setup wizard appears. Follow the steps to install Bitdefender Ultimate Small Business Security.

Step 1 - Bitdefender Installation

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

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

Two additional tasks can be performed at this step:

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

❍ Select the language you want to install the product in.

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

Step 2 - Installation in process

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

Step 3 - Installation completed

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

Step 4 - Device Analysis

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

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

When the scan is completed, click **Continue with Create Account**.

> (i) Note
> Alternatively, if you do not wish to perform the scan, you can simply click on **Skip**.

Step 5 - Bitdefender account

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

Proceed according to your situation.

❍ **I want to create a Bitdefender account**

1. Type the required information in the corresponding fields. The data you provide here will remain confidential. The password must be at least 8 characters long, include at least one number or symbol and include lower and upper case characters.

2. Before proceeding further you have to agree with the Terms of use. Access the Terms of use and read them carefully as they contain the terms and conditions under which you may use Bitdefender. Additionally, you can access and read the Privacy Policy.

3. Click **CREATE ACCOUNT**.

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

❍ **I already have a Bitdefender account**

1. Click **Sign In**.

2. Type the email address in the corresponding field, and then click **NEXT**.

3. Type your password, and then click **SIGN IN**.
   If you forgot the password for your account or you simply want to reset the one you already set:

   a. Click **Forgot password?**.

   b. Type your email address, and then click **NEXT**.

   c. Check your email account, type the security code you have received, and then click **NEXT**.
   Alternatively, you can click **Change password** in the email that we sent you.

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

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

❍ **I want to sign in using my Microsoft, Facebook or Google account**
To sign in with your Microsoft, Facebook or Google account:

1. Select the service you want to use. You will be redirected to the login page of that service.

2. Follow the instructions provided by the selected service to link your account to Bitdefender.

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

Step 6 - Activate your product

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

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

Proceed according to your situation:

❍ I have an activation code
In this case, activate the product by following these steps:

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

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

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

Step 7 - Get started

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

Click **FINISH** to access the Bitdefender Ultimate Small Business Security interface.

3.2. Managing your Security

3.2.1. Antivirus protection

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

❍ On-access scanning - prevents new threats from entering your system. Bitdefender will, for example, scan a word document for known threats when you open it, and an email message when you receive one.
On-access scanning ensures real-time protection against threats, being an essential component of any computer security program.

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

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

Bitdefender automatically scans any removable media that is connected to the device to make sure it can be safely accessed. For more information, refer to Automatic scan of removable media (page 32).

Advanced users can configure scan exceptions if they do not want specific files or file types to be scanned. For more information, refer to Configuring scan exceptions (page 34).

When it detects a threat, Bitdefender will automatically attempt to remove the malicious code from the infected file and reconstruct the original file. This operation is referred to as disinfection. Files that cannot be disinfected are moved to quarantine to contain the infection. For more information, refer to Managing quarantined files (page 36).

If your device has been infected with threats, refer to Removing threats from your system (page 135). To help you clean your device of threats that cannot be removed from within the Windows operating system, Bitdefender provides you with Rescue Environment (page 135). This is a trusted environment, especially designed for threat removal, which enables you to boot your device independent of Windows. When the device runs in Rescue Environment, Windows threats are inactive, making it easy to remove them.

On-access scanning (real-time protection)

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

Turning on or off real-time protection

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

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. In the **Advanced** window, turn on or off **Bitdefender Shield**.

4. If you want to disable real-time protection, a warning window appears. You must confirm your choice by selecting from the menu how long you want the real-time protection to be disabled. You can disable real-time protection for 5, 15 or 30 minutes, for an hour, permanently or until a system restart. The real-time protection will automatically turn on when the selected time will expire.

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

Configuring the real-time protection advanced settings

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

To configure the real-time protection advanced settings:

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. In the **Advanced** window, you can configure the scan settings as needed.

Information on the scan options

You may find this information useful:

❍ **Scan only applications.** You can set Bitdefender to scan only accessed apps.

❍ **Scan potentially unwanted applications.** Select this option to scan for unwanted applications. A potentially unwanted application (PUA) or potentially unwanted program (PUP) is a software that usually comes bundled with freeware software and will display pop-ups or install a toolbar in the default browser. Some of them will change the homepage or the search engine, others will run several processes in the background slowing down the PC or will display numerous ads. These programs can be installed without your consent (also called adware) or will be included by default in the express installation kit (ad-supported).

❍ **Scan scripts.** The Scan scripts feature allows Bitdefender to scan powershell scripts and office documents that could contain script-based malware.

❍ **Scan network shares.** To safely access a remote network from your device, we recommend you to keep the Scan network shares option enabled.

❍ **Scan process memory.** Scans for malicious activity in the memory of running processes.

❍ **Scan command line.** Scans the command line of newly launched applications to prevent fileless attacks.

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

If you decide on using this option, turn it on, and then drag the slider along the scale to exclude from scanning archives that are bigger than a given value in MB (Megabytes).

❍ **Scan boot sectors.** You can set Bitdefender to scan the boot sectors of your hard disk. This sector of the hard disk contains the necessary computer code to start the boot process. When a threat infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.

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

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

❍ **Early boot scan.** Select the **Early boot scan** option to scan your system at startup as soon as all its critical services are loaded. The mission of this feature is to improve threat detection at system startup and the boot time of your system.

Actions taken on detected threats

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

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. In the **Advanced** window, scroll down on the window until you see the **Threat actions** option.

4. Configure the scan settings as needed.

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

Take proper action

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

❍ **Infected files.** Files detected as infected match a piece of threat information found in the Bitdefender Threat Information Database. Bitdefender will automatically attempt to remove the malicious code from the infected file and reconstruct the original file. This operation is referred to as disinfection.

Files that cannot be disinfected are moved to quarantine to contain the infection. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. For more information, refer to Managing quarantined files (page 36).

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

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

❍ **Archives containing infected files.**

❍ Archives that contain only infected files are deleted automatically.

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

Move to quarantine

Moves detected files to quarantine. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. For more information, refer to Managing quarantined files (page 36).

Deny access

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

Restoring the default settings

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

To restore the default real-time protection settings:

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. In the **Advanced** window, scroll down on the window until your see the **Reset advanced settings** option. Select this option to reset the antivirus settings to default.

On-demand scanning

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

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

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

Scanning a file or folder for threats

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

Running a Quick Scan

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

To run a Quick Scan:

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. In the **Scans** windows, click the **Run Scan** button next to **Quick Scan**.

4. Follow the Antivirus Scan wizard to complete the scan. Bitdefender will automatically take the recommended actions on detected files. If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

Running a System Scan

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

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

Before running a System Scan, the following are recommended:

❍ Make sure Bitdefender is up-to-date with its threat information database. Scanning your device using an outdated threat information database may prevent Bitdefender from detecting new threats found since the last update. For more information, refer to Keeping Bitdefender up-to-date.

❍ Shut down all open programs.

If you want to scan specific locations on your device or to configure the scanning options, configure and run a custom scan. For more information, refer to Configuring a custom scan (page 26).

To run a System Scan:

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. In the **Scans** windows, click the **Run Scan** button next to **System Scan**.

4. The first time you run a System Scan, you are introduced into the feature. Click **Ok, got it** to continue.

5. Follow the Antivirus Scan wizard to complete the scan. Bitdefender will automatically take the recommended actions on detected files. If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

Configuring a custom scan

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

To configure a new custom scan in detail:

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. In the **Scans** windows, click **+Create scan**.

4. In the **Task Name** field, type a name for the scan, then select the locations you would like to be scanned, and then click **Next**.

5. Configure these general options:

   ❍ **Scan only applications.** You can set Bitdefender to scan only accessed apps.

   ❍ **Scan task priority.** You can choose the impact a scan process should have on your system performance.

      ❍ Auto - The priority of the scan process will depend on the system activity. To make sure that the scan process will not affect the system activity, Bitdefender will decide whether the scan process should be run with high or low priority.

      ❍ High - The priority of the scan process will be high. By choosing this option, you will allow other programs to run slower and decrease the time needed for the scan process to finish.

      ❍ Low - The priority of the scan process will be low. By choosing this option, you will allow other programs to run faster and increase the time needed for the scan process to finish.

   ❍ **Post scan actions.** Choose what action Bitdefender should take in case no threats are found:

❍ Show Summary window

❍ Shutdown device

❍ Close Scan window

6. If you want to configure the scanning options in detail, click **Show advanced options**. You can find information about the listed scans at the end of this section.
Click **Next**.

7. You can enable **Schedule scan task** if you wish, and then choose when the custom scan you created should start.

❍ At system startup

❍ Daily

❍ Monthly

❍ Weekly

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

8. Click **Save** to save the settings and close the configuration window.
Depending on the locations to be scanned, the scan may take a while. If threats will be found during the scanning process, you will be prompted to choose the actions to be taken on the detected files.

Information on the scan options

You may find this information useful:

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

❍ **Scan potentially unwanted applications.** Select this option to scan for unwanted applications. A potentially unwanted application (PUA) or potentially unwanted program (PUP) is a software that usually comes bundled with freeware software and will display pop-ups or install a toolbar in the default browser. Some of them will change the homepage or the search engine, others will run several processes in the background slowing down the PC or will display numerous ads. These programs can be installed without your consent (also called

adware) or will be included by default in the express installation kit (ad-supported).

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

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

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

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

❍ **Scan boot sectors.** You can set Bitdefender to scan the boot sectors of your hard disk. This sector of the hard disk contains the necessary computer code to start the boot process. When a threat infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.

❍ **Scan memory.** Select this option to scan programs running in your system's memory.

❍ **Scan registry.** Select this option to scan registry keys. Windows Registry is a database that stores configuration settings and options for the Windows operating system components, as well as for installed apps.

❍ **Scan cookies.** Select this option to scan the cookies stored by browsers on your device.

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

Antivirus Scan Wizard

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

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

Step 1 - Perform scan

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

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

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

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

❍ **Password.** If you want Bitdefender to scan the archive, select this option and type the password. If you do not know the password, choose one of the other options.

❍ **Don't ask for a password and skip this object from scan.** Select this option to skip scanning this archive.

❍ **Skip all password-protected items without scanning them.** Select this option if you do not want to be bothered about password-protected archives. Bitdefender will not be able to scan them, but a record will be kept in the scan log.

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

Step 2 - Choose actions

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

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

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

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

Take proper actions

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

❍ **Infected files.** Files detected as infected match a piece of threat information found in the Bitdefender Threat Information Database. Bitdefender will automatically attempt to remove the malicious code from the infected file and reconstruct the original file. This operation is referred to as disinfection.
Files that cannot be disinfected are moved to quarantine to contain the infection. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. For more information, refer to Managing quarantined files (page 36).

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

❍ **Suspicious files.** Files are detected as suspicious by the heuristic analysis. Suspicious files cannot be disinfected, because no

disinfection routine is available. They will be moved to quarantine to prevent a potential infection.

❍ **Archives containing infected files.**

    ❍ Archives that contain only infected files are deleted automatically.

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

Delete

Removes detected files from the disk.

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

Take no action

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

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

Step 3 - Summary

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

> ⚠ Important
>
> In most cases Bitdefender successfully disinfects the infected files it detects or it isolates the infection. However, there are issues that cannot be solved automatically. If required, restart your system to complete the cleaning process. For more information and instructions on how to remove a threat manually, refer to Removing threats from your system (page 135).

Checking scan logs

Each time a scan is performed, a scan log is created and Bitdefender records the detected issues in the Antivirus window. The scan log contains detailed information about the logged scanning process, such as scanning options, the scanning target, the threats found and the actions taken on these threats.

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

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

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

2. In the **All** tab, select the notification regarding the latest scan.
   This is where you can find all threat scan events, including threats detected by on-access scanning, user-initiated scans and status changes for automatic scans.

3. In the notifications list, you can check what scans have been performed recently. Click a notification to view details about it.

4. To open the scan log, click **View log**.

Automatic scan of removable media

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

Detected devices fall into one of these categories:

❍ CDs/DVDs

❍ Flash drives, such as flash pens and external hard-drives

❍ mapped (remote) network drives

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

How does it work?

When it detects a removable storage device, Bitdefender starts scanning it for threats (provided automatic scan is enabled for that type of device).

You will be notified through a pop-up window that a new device has been detected and it is being scanned.

A Bitdefender scan 🅱 icon will appear in the system tray. You can click this icon to open the scan window and to see the scan progress.

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

In most cases, Bitdefender automatically removes detected threats or isolates infected files into quarantine. If there are unresolved threats after the scan, you will be prompted to choose the actions to be taken on them.

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

This information may be useful to you:

❍ Be careful when using a threat-infected CD/DVD, because the threat cannot be removed from the disc (the media is read-only). Make sure real-time protection is turned on to prevent threats from spreading to your system. It is best practice to copy any valuable data from the disc to your system, and then dispose of the disc.

❍ In some cases, Bitdefender may not be able to remove threats from specific files due to legal or technical constraints. Such an example are files archived using a proprietary technology (this is because the archive cannot be recreated correctly).
To find out how to deal with threats, refer to Removing threats from your system (page 135).

Managing removable media scan

To manage automatic scan of removable media:

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. Select the **Settings** window.

The scanning options are pre-configured for the best detection results. If infected files are detected, Bitdefender will try to disinfect them (remove the malicious code) or to move them to quarantine. If both actions fail, the

Antivirus Scan wizard will allow you to specify other actions to be taken on infected files. The scanning options are standard and you cannot change them.

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

Scan hosts file

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

To configure scan hosts file:

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

2. Select the **Advanced** tab.

3. Turn on or off **Scan hosts file**.

Configuring scan exceptions

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

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

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

Excepting files and folders from scanning

To except specific files and folders from scanning:

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. In the **Settings** window, click **Manage Exceptions**.

4. Click **+Add an Exception**.

5. Enter the path of the folder you want to except from scanning in the corresponding field.
Alternatively, you can navigate to the folder by clicking the browse button in the right side of the interface, select it and click on **OK**.

6. Turn on the switch next to the protection feature that should not scan the folder. There are three options:

   ❍ Antivirus

   ❍ Online Threat Prevention

   ❍ Advanced Threat Defense

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

Excepting files extensions from scanning

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

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

To except file extensions from scanning:

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. In the **Settings** window, click **Manage Exceptions**.

4. Click **+Add an Exception**.

5. Type the extensions that you want to be excepted from scanning with a dot before them, separating them with semicolons (;).
txt;avi;jpg

6. Turn on the switch next to the protection feature that should not scan the extension.

7. Click **Save**.

Managing scan exceptions

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

To manage scan exceptions:

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. In the **Settings** window, click **Manage Exceptions**. A list with all your exceptions will be displayed.

4. To remove or edit scan exceptions, click one of the available buttons. Proceed as follows:

   ❍ To remove an entry from the list, click the 🗑 button next to it.

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

Managing quarantined files

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

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

To check and manage quarantined files:

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. Go to the **Settings** window.
   Here you can view the name of the quarantined files, their original location and the name of the detected threats.

4. Quarantined files are managed automatically by Bitdefender according to the default quarantine settings.

Though not recommended, you can adjust the quarantine settings according to your preferences by clicking **View Settings**.

Click the switches to turn on or off:

Rescan quarantine after threat information update

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

Delete content older than 30 days

Quarantined files older than 30 days are automatically deleted.

Create exceptions for restored files

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

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

3.2.2. Advanced Threat Defense

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

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

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

Turning on or off Advanced Threat Defense

To turn on or off Advanced Threat Defense:

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

2. In the **ADVANCED THREAT DEFENSE** pane, click **Open**.

3. Go to the **Settings** window and click switch next to **Bitdefender Advanced Threat Defense**.

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

Checking detected malicious attacks

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

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

2. In the **ADVANCED THREAT DEFENSE** pane, click **Open**.

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

Adding processes to exceptions

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

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

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

2. In the **ADVANCED THREAT DEFENSE** pane, click **Open**.

3. In the **Settings** window, click **Manage Exceptions**.

4. Click **+Add an Exception**.

5. Enter the path of the folder you want to except from scanning in the corresponding field.
   Alternatively, you can navigate to the executable by clicking the browse button in the right side of the interface, select it and click on **OK**.

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

7. Click **Save**.

Exploits detection

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

Turning on or off exploit detection

To turn on or off the exploit detection:

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

❍ In the **ADVANCED THREAT DEFENSE** pane, click **Open**.

❍ Go to the **Settings** window and click the switch next to **Exploit detection** to turn the feature on or off.

> ⓘ Note
> The Exploit detection option is enabled by default.

3.2.3. Online Threat Prevention

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

Bitdefender provides real-time online threat prevention for:

❍ Internet Explorer

❍ Microsoft Edge

❍ Mozilla Firefox

❍ Google Chrome

❍ Safari

❍ Bitdefender Safepay™

❍ Opera

To configure Online Threat Prevention settings:

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

2. In the **ONLINE THREAT PREVENTION** pane, click **Settings**.

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

❍ Web attack prevention blocks threats coming from the internet, including drive-by downloads.

❍ Search Advisor, a component that rates the results of your search engine queries and the links posted on social networking websites by placing an icon next to every result:

🔴 You should not visit this webpage.

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

🟢 This is a safe page to visit.

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

   ❍ Google

   ❍ Yahoo!

   ❍ Bing

   ❍ Baidu

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

   ❍ Facebook

   ❍ Twitter

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

❍ Fraud protection.

❍ Phishing protection.

Scroll down and you will reach the **Network threat prevention** section. Here you have the **Network threat prevention** option. To keep your device away from attacks made by complex malware (such as ransomware) through the exploitation of vulnerabilities, keep this option enabled.

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

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

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

2. In the **ONLINE THREAT PREVENTION** pane, click **Settings**.

3. Click **Manage exceptions**.

4. Click **+Add an Exception**.

5. Type in the corresponding field the name of the website, the name of the domain, or the IP address you want to add to exceptions.

6. Click the switch next to **Online Threat Prevention**.

7. To remove an entry from the list, click the 🗑 button next to it.
   Click **Save** to save the changes and close the window.

Bitdefender alerts in the browser

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

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

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

❍ Navigate away from the website by clicking **TAKE ME BACK TO SAFETY**.

❍ Proceed to the website, despite the warning, by clicking **I understand the risks, take me there anyway**.

❍ If you are sure that the detected website is safe, click **SUBMIT** to add it to exceptions. We recommend you to add only websites that you fully trust.

3.2.4. Email Protection

Your email is an important part of your digital life, and given its multiple applications in real life, it has become a preferred attack vector for bad actors and one of the primary cybersecurity concerns of the everyday user.

Email Protection is a security feature that allows you to scan and identify potentially dangerous content in emails received in your inbox.

This feature is a package of a variety of technologies brought together under the same protection module, such as anti-phishing, antimalware, antispam, anti-fraud and anti-scam software.

By creating a direct connection between Bitdefender and your email service provider, you allow the antivirus to scan your emails directly and eliminate the limitations incurred by using different devices or email clients.

> **Note**
> You can protect up to 5 different email accounts.

Configuring your account

This feature is seamlessly integrated into the user interface. To start using Email Protection:

1. Under **Protection**, click **Open** in the **Email Protection** card.

2. Choose your email provider for the email account you want to protect.

> **Note**
> Email Protection is currently available for Google accounts, Outlook accounts and soon-to-be available for Yahoo Mail as well.

3. Click on the **Sign in** button.
   The operation will then continue in your browser.

4. Enter your email address and click on the **Next** button

5. To continue, enter your passowrd and click on the **Next** button.

6. Check the permissions requested on screen and allow Bitdefender to protect your email account.

Your email account is now protected and all your newly incoming emails will be scanned against threats.

> **Note**
> Each scanned email will be marked with a label to indicate its safetly levels.

Dashboard

The dashboard will display your protected emails under which you will find:

❍ configuration date (the date at which the account was set up for Email Protection)

❍ status (active or inactive)

❍ number of filtered emails in the last 30 days.
Here you will see a chart showcasing the number of safe emails and dangerous emails received.

To add multiple email accounts click on the **Add another account** and go through the configuration process above for each of them.

To pause scanning or remove an account from this feature click on the three dots next to the account in question and click of **Manage account**.

3.2.5. Antispam

Spam is a term used to describe unsolicited email. Spam is a growing problem, both for individuals and for organizations. It's not pretty, you wouldn't want your kids to see it, it can get you fired (for wasting too much time or from receiving porn in your office mail) and you can't stop people from sending it. The next best thing to that is, obviously, to stop receiving it. Unfortunately, Spam comes in a wide range of shapes and sizes, and there's a lot of it.

Bitdefender Antispam employs remarkable technological innovations and industry standard antispam filters to weed out spam before it reaches the user's Inbox. For more information, refer to Antispam insights (page 44).

The Bitdefender Antispam protection is available only for email clients configured to receive email messages via the POP3 protocol. POP3 is one of the most widely used protocols for downloading email messages from a mail server.

> ⓘ **Note**
> Bitdefender does not provide antispam protection for email accounts that you access through a web-based email service.

The spam messages detected by Bitdefender are marked with the [spam] prefix in the subject line. Bitdefender automatically moves spam messages to a specific folder, as follows:

❍ In Microsoft Outlook, spam messages are moved to a **Spam** folder, located in the **Deleted Items** folder. The **Spam** folder is created when an email is labeled as spam.

❍ In Mozilla Thunderbird, spam messages are moved to a **Spam** folder, located in the **Trash** folder. The **Spam** folder is created when an email is labeled as spam.

If you use other mail clients, you must create a rule to move the email messages marked as [spam] by Bitdefender to a custom quarantine folder. If the Deleted items or Trash folders are deleted, the Spam folder will be deleted too. However, a new Spam folder will be created as soon as an email is labeled as spam.

Antispam insights

The antispam feature has the following features and settings:

Antispam filters

The Bitdefender Antispam Engine incorporates cloud protection and other several different filters that ensure your Inbox to be SPAM-free, like Friends list, Spammers list and Charset filter.

Friends list / Spammers list

Most people communicate regularly to a group of people or even receive messages from companies or organizations in the same domain. By using **friends or spammers list**, you can easily classify which people you want to receive email from (friends) no matter what the message contains, or which people you never want to hear from again (spammers).

> **i** Note
>
> We recommend that you add your friends' names and email addresses to the **Friends list**. Bitdefender does not block messages from those on the list; therefore, adding friends helps ensure that legitimate messages get through.

Charset filter

Many spam messages are written in Cyrillic and / or Asian charsets. The Charset Filter detects this kind of messages and tags them as SPAM.

Antispam operation

The Bitdefender Antispam Engine uses all antispam filters combined to determine whether a certain email message should get into your **Inbox** or not.

Every email that comes from the internet is first checked with the Friends list/Spammers list filter. If the sender's address is found in the Friends list the email is moved directly to your **Inbox**.

Otherwise, the Spammers list filter will take over the email to verify if the sender's address is on its list. If a match is made, the email will be tagged as SPAM and moved in the **Spam** folder.

Else, the Charset filter will check if the email is written in Cyrillic or Asian characters. If so the email will be tagged as SPAM and moved in the **Spam** folder.

> ⓘ Note
> If the email is tagged as SEXUALLY EXPLICIT in the subject line, Bitdefender will consider it SPAM.

Supported email clients and protocols

Antispam protection is provided for all POP3/SMTP email clients. The Bitdefender Antispam toolbar however is integrated only into:

❍ Microsoft Outlook 2007 / 2010 / 2013 / 2016 / 2019

❍ Mozilla Thunderbird 14 and higher versions

Turning on or off antispam protection

Antispam protection is enabled by default.

To turn on or off the Antispam feature:

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

2. In the **ANTISPAM** pane, turn on or off the switch.

Using the antispam toolbar in your mail client window

In the upper area of your mail client window you can see the Antispam toolbar. The Antispam toolbar helps you manage antispam protection directly from your mail client. You can easily correct Bitdefender if it marked a legitimate message as SPAM.

> ⚠ Important
> Bitdefender integrates into the most commonly used mail clients through an easy-to-use antispam toolbar. For a complete list of supported mail clients, refer to Supported email clients and protocols (page 45).

Each button from the Bitdefender toolbar will be explained below:

⚙ **Settings** - opens a window where you can configure the antispam filters and the toolbar settings.

🔖 **Is Spam** - indicates that the selected email is spam. The email will be moved immediately to the **Spam** folder. If the antispam cloud services are activated, the message is sent to Bitdefender Cloud for further analysis.

🔖 **Not Spam** - indicates that the selected email is not spam and Bitdefender should not have tagged it. The email will be moved from the **Spam** folder to the **Inbox** directory. If the antispam cloud services are activated, the message is sent to Bitdefender Cloud for further analysis.

> ⚠ Important
>
> The 🔖 **Not Spam** button becomes active when you select a message marked as SPAM by Bitdefender (normally these messages are located in the **Spam** folder).

👤 **Add Spammer** - adds the sender of the selected email to the Spammers list. You may need to click **OK** to acknowledge. The email messages received from addresses in the Spammers list are automatically marked as [spam].

👤 **Add Friend** - adds the sender of the selected email to the Friends list. You may need to click **OK** to acknowledge. You will always receive email messages from this address no matter what they contain.

👤 **Spammers** - opens the **Spammers list** that contains all the email addresses from which you don't want to receive messages, regardless of their content. For more information, refer to Configuring the Spammers List (page 49).

👤 **Friends** - opens the **Friends list** that contains all the email addresses from which you always want to receive email messages, regardless of their content. For more information, refer to Configuring the Friends List (page 48).

Indicating detection errors

If you are using a supported mail client, you can easily correct the antispam filter (by indicating which email messages should not have been marked as [spam]). Doing so helps improve the efficiency of the antispam filter. Follow these steps:

1. Open your mail client.

2. Go to the junk mail folder where spam messages are moved.

3. Select the legitimate message incorrectly marked as [spam] by Bitdefender.

4. Click ⬇ the **Add Friend** button on the Bitdefender antispam toolbar to add the sender to the Friends list. You may need to click **OK** to acknowledge. You will always receive email messages from this address no matter what they contain.

5. Click the ⬇ **Not Spam** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window). The email message will be moved to the Inbox folder.

Indicating undetected spam messages

If you are using a supported mail client, you can easily indicate which email messages should have been detected as spam. Doing so helps improve the efficiency of the antispam filter. Follow these steps:

1. Open your mail client.

2. Go to the Inbox folder.

3. Select the undetected spam messages.

4. Click the ⬇ **Is Spam** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window). They are immediately marked as [spam] and moved to the junk mail folder.

Configuring toolbar settings

To configure the antispam toolbar settings for your email client, click ⚙ **Settings** button on the toolbar, and then the **Toolbar Settings** tab.

Here you have the following options:

❍ **Mark spam email messages as 'Read'** - marks the spam messages as read automatically, so as not to be disturbing when they arrive.

❍ You can choose whether or not to display confirmation windows when you click the ⬇ **Add Spammer** and ⬇ **Add Friend** buttons on the antispam toolbar.

Confirmation windows can prevent accidentally adding email senders to Friends / Spammers list.

Configuring the Friends List

The **Friends list** is a list of all the email addresses from which you always want to receive messages, regardless of their content. Messages from your friends are not labeled as spam, even if the content resembles spam.

> **ⓘ Note**
> Any mail coming from an address contained in the **Friends list**, will automatically be delivered to your Inbox without further processing.

To configure and manage the Friends list:

❍ If you are using Microsoft Outlook or Thunderbird, click the 🔧 Friends button on the Bitdefender antispam toolbar.

❍ Alternatively:

1. Click **Protection** on the navigation menu on the Bitdefender interface.
2. In the **ANTISPAM** pane, click **Settings**.
3. Access the **Manage Friends** window.

To add an email address, select the **Email address** option, enter the address, and then click **ADD**. Syntax: name@domain.com.

To add all the email addresses from a specific domain, select the **Domain name** option, enter the domain name, and then click **ADD**. Syntax:

❍ @domain.com and domain.com - all the received email messages from domain.com will reach your **Inbox** regardless of their content;

❍ domain - all the received email messages from domain (no matter the domain suffixes) will be tagged as SPAM;

❍ com - all the received email messages having the domain suffix com will be tagged as SPAM;

It is recommended to avoid adding entire domains, but this may be useful in some situations. For example, you can add the email domain of the company you work for, or those of your trusted partners.

To delete an item from the list, click the corresponding 🗑 button next to it. To delete all entries from the list, click **Clear List**.

You can save the Friends list to a file so that you can use it on another device or after reinstalling the product. To save the Friends list, click the Save button and save it to the desired location. The file will have a .bwl extension.

To load a previously saved Friends list, click **Load** and open the corresponding .bwl file. To reset the content of the existing list when loading a previously saved list, check the box next to **Overwrite current list**.

Configuring the Spammers List

The **Spammers list** is a list of all the email addresses from which you don't want to receive messages, regardless of their content. Any email message received from an address contained in the **Spammers list** will be automatically marked as SPAM, without further processing.

To configure and manage the Spammers list:

❍ If you are using Microsoft Outlook or Thunderbird, click 👤 **Spammers** button on the Bitdefender antispam toolbar integrated into your mail client.

❍ Alternatively:

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

2. In the **ANTISPAM** pane, click **Settings**.

3. Access the **Manage Spammers** window.

To add an email address, select the **Email address** option, enter the address, and then click **ADD**. Syntax: name@domain.com.

To add all the email addresses from a specific domain, select the **Domain name** option, enter the domain name, and then click **ADD**. Syntax:

❍ @domain.comand domain.com - all the received email messages from domain.com will reach your **Inbox** regardless of their content;

❍ domain - all the received email messages from domain (no matter the domain suffixes) will be tagged as SPAM;

❍ com - all the received email messages having the domain suffix com will be tagged as SPAM.

It is recommended to avoid adding entire domains, but this may be useful in some situations.

> ### ⊗ Warning
> Do not add domains of legitimate web-based email services (such as Yahoo, Gmail, Hotmail or other) to the Spammers list. Otherwise, the email messages received from any registered user of such a service will be detected as spam. If, for example, you add yahoo.com to the Spammers list, all email messages coming from yahoo.com addresses will be marked as [spam].

To delete an item from the list, click the corresponding 🗑 button next to it. To delete all entries from the list, click **Clear List**.

You can save the Spammers list to a file so that you can use it on another device or after reinstalling the product. To save the Spammers list, click the **Save** button and save it to the desired location. The file will have a *.bwl* extension.

To load a previously saved Spammers list, click **LOAD** and open the corresponding .bwl file. To reset the content of the existing list when loading a previously saved list, select Overwrite current list.

Configuring the local antispam filters

As described in Antispam insights (page 44), Bitdefender uses a combination of different antispam filters to identify spam. The antispam filters are pre-configured for efficient protection.

> ### ⚠ Important
> Depending on whether or not you receive legitimate emails written in Asian or Cyrillic characters, disable or enable the setting that automatically blocks such emails. The corresponding setting is disabled in the localized versions of the program that use such charsets (for example, in the Russian or Chinese version).

To configure the local antispam filters:

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

2. In the **ANTISPAM** pane, click **Settings**.

3. Go to the **Settings** window and click the corresponding turn on or off switches.

If you are using Microsoft Outlook or Thunderbird, you can configure the local antispam filters directly from your mail client. Click the ⚙ **Settings**

button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window), and then the **Antispam Filters** tab.

Configuring the cloud settings

The cloud detection makes use of the Bitdefender Cloud services to provide you with efficient and always up-to-date antispam protection.

The cloud protection functions as long as you keep Bitdefender Antispam enabled.

Samples of legitimate or spam emails can be submitted to Bitdefender Cloud when you indicate detection errors or undetected spam emails. This helps improve the Bitdefender antispam detection.

Configure the email sample submission to Bitdefender Cloud by selecting the desired options by following these steps:

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

2. In the **ANTISPAM** pane, click **Settings**.

3. Go to the **Settings** window and click the corresponding turn on or off switches.

If you are using Microsoft Outlook or Thunderbird, you can configure the cloud detection directly from your mail client. Click the ⚙ **Settings** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window), and then the **Cloud Settings** tab.

3.2.6. Firewall

> **Note**
> The Firewall module within Bitdefender Ultimate Small Business Security will be turned off by default. You will have to enable it manually.
>
> If **Windows Defender Firewall** is enabled during this procedure, you will be prompted to disable it first.

The Firewall protects your device from inbound and outbound unauthorized connection attempts, both on local networks and on the internet. It is quite similar to a guard at your gate - it keeps track of connection attempts and decides which to allow and which to block.

The Bitdefender firewall uses a set of rules to filter data transmitted to and from your system.

Under normal conditions, Bitdefender automatically creates a rule whenever an app tries to access the internet. You can also manually add or edit rules for apps.

As a safety measure you will be notified each time a potentially malicious app is blocked from accessing the internet.

Bitdefender automatically assigns a network type to every network connection it detects. Depending on the network type, the firewall protection is set to the appropriate level for each connection.

To find out more about the firewall settings for each network type and how you can edit the network settings, refer to Managing connection settings (page 55).

Turning on or off firewall protection

To turn firewall protection on or off:

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

2. In the **FIREWALL** pane, turn on or off the switch.

> Warning
>
> Because it exposes your device to unauthorized connections, turning off the firewall should only be a temporary measure. Turn the firewall back on as soon as possible.

Managing app rules

To view and manage the firewall rules controlling apps' access to network resources and the internet:

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

2. In the **FIREWALL** pane, click **Settings**.

3. Go to the **Application Access** window.

You can see the latest programs (processes) that have passed through Bitdefender Firewall and the internet network you are connected to. To see the rules created for a specific app, simply click it, and then click the **View application rules** link. The **Rules** window opens.

For each rule the following information is displayed:

❍   **NETWORK** - the process and the network adapter types (Home / Office, Public or All) to which the rule applies to. Rules are

automatically created to filter network or internet access through any adapter. By default, the rules apply to any network. You can manually create rules or edit existing rules to filter an app's network or internet access through a specific adapter (for example, a wireless network adapter).

❍ **PROTOCOL** - the IP protocol the rule applies to. By default, the rules apply to any protocol.

❍ **TRAFFIC** - the rule applies in both directions, inbound and outbound.

❍ **PORTS** - the PORT protocol the rule applies to. By default, the rules apply to all ports.

❍ **IP** - the internet protocol (IP) the rule applies to. By default, the rules apply to any IP address.

❍ **ACCESS** - whether the app is allowed or denied access to the network or internet under the specified circumstances.

To edit or delete the rules for the selected app, click the ⋯ icon.

❍ **Edit rule** - opens a window where you can edit the current rule.

❍ **Delete rule** - you can choose to remove the current set of rules for the selected app.

Adding app rules

To add an app rule:

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

2. In the **FIREWALL** pane, click **Settings**.

3. In the **Rules** window, click **Add rule**.

Here you can apply the following changes:

❍ **Apply this rule to all applications.** Enable this switch to apply the created rule to all apps.

❍ **Program Path.** Click **BROWSE** and select the app the rule applies to.

❍ **Permission.** Select one of the available permissions:

Permission	Description
Allow	The specified app will be allowed network / internet access under the specified circumstances.

Permission	Description
Deny	The specified app will be denied network / internet access under the specified circumstances.

❍ **Network Type**. Select the type of network the rule applies to. You can change the type by opening the **Network Type** drop-down menu and selecting one of the available types from the list.

Network Type	Description
Any Network	Allow all traffic between your device and other devices no matter the network type.
Home/Office	Allow all traffic between your device and different ones in the local network.
Public	All traffic is filtered.

❍ **Protocol.** Select from the menu the IP protocol the rule applies to.

 ❍ If you want the rule to apply to all protocols, select **Any**.

 ❍ If you want the rule to apply to TCP, select **TCP**.

 ❍ If you want the rule to apply to UDP, select **UDP**.

 ❍ If you want the rule to apply to ICMP, select **ICMP**.

 ❍ If you want the rule to apply to IGMP, select **IGMP**.

 ❍ If you want the rule to apply to GRE, select **GRE**.

 ❍ If you want the rule to apply to a specific protocol, type the number assigned to the protocol you want to filter in the blank edit field.

> **i** Note
> IP protocol numbers are assigned by the Internet Assigned Numbers Authority (IANA). You can find the complete list of assigned IP protocol numbers at http://www.iana.org/assignments/protocol-numbers.

❍ **Direction.** Select from the menu the traffic direction the rule applies to.

Direction	Description
Outbound	The rule applies only for the outgoing traffic.
Inbound	The rule applies only for the incoming traffic.
Both	The rule applies in both directions.

Click the **Advanced Settings** button in the lower part of the window to customize the following settings:

❍ **Custom Local Address.** Specify the local IP address and port the rule applies to.

❍ **Custom Remote Address.** Specify the remote IP address and port the rule applies to.

To remove the current set of rules and restore the default ones, click **Reset rules** in the **Rules** window.

Managing connection settings

Whether you connect to the internet using a Wi-Fi or Ethernet adapter, you can configure what settings should be applied for a safe navigation. The options you can choose from, are:

❍ **Dynamic** – the network type will be automatically set based on the profile of the connected network, Home/Office or Public. When this happens, only Firewall rules for the specific network type or those defined to apply to all network types will apply.

❍ **Home / Office** – the network type will always be Home / Office, disregarding the profile of the connected network. When this happens, only Firewall rules for Home/Office or those defined to apply to all network types will apply.

❍ **Public** - the network type will always be Public, disregarding the profile of the connected network. When this happens, only Firewall rules for Public or those defined to apply to all network types will apply.

To configure your network adapters:

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

2. In the **FIREWALL** pane, click **Settings**.

3. Select the **Network Adapters** window.

4. Select the settings you want to apply when connecting to the following adapters:

   ❍ Wi-Fi

   ❍ Ethernet

Configuring advanced settings

To configure advanced firewall settings:

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

2. In the **FIREWALL** pane, click **Settings**.

3. Select the **Settings** window.

The following features can be configured:

❍ **Port scan protection** - detects and blocks attempts to find out which ports are open.
Port scans are frequently used by hackers to find out which ports are open on your device. They might then break into your device if they find a less secure or vulnerable port.

❍ **Alert mode** - alerts are shown each time an app tries to connect to the internet. Select **Allow** or **Block**. When Alert mode is turned on, the Profiles feature is automatically switched off. Alert mode can be used simultaneously with **Battery Mode**.

❍ **Allow access to domain network** - allow or deny access to resources and shares defined by your domain controllers.

❍ **Stealth Mode** - whether you can be detected by other devices. Click the **Edit stealth settings** to choose when your device should or should not be visible to other devices.

❍ **Default application behavior** - allow Bitdefender apply automatic settings to app with no defined rules. Click **Edit default rules** to choose whether automatic settings should be applied or not.

   ❍ Automatic - apps access will be allowed or denied based on the automatic Firewall and user rules.

   ❍ Allow - apps that don't have any Firewall rule defined will be automatically allowed.

   ❍ Block - apps that don't have any Firewall rule defined will be automatically blocked.

3.2.7. Vulnerability

An important step in protecting your device against malicious actions and apps is to keep the operating system and the apps you regularly use up

to date. Moreover, to prevent unauthorized physical access to your device, strong passwords (passwords that cannot be easily guessed) must be configured for each Windows user account and for the Wi-Fi networks you connect to as well.

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

❍ You can scan your system for vulnerabilities and fix them step by step using the **Vulnerability Scan** option.

❍ Using automatic vulnerability monitoring, you can check and fix detected vulnerabilities in the Notifications window.

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

Scanning your system for vulnerabilities

To detect system vulnerabilities, Bitdefender requires an active internet connection.

To scan you system for vulnerabilities:

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

2. In the **VULNERABILITY** pane, click **Open**.

3. In the **Vulnerability Scan** tab click **Start Scan**, then wait for Bitdefender to check your system for vulnerabilities. The detected vulnerabilities are grouped in the three categories:

   ❍ **OPERATING SYSTEM**

      ❍ **Operating System Security**
      Altered system settings that may compromise your device and data, such as not displaying warnings when executed files perform changes on your system without your permission or when MTP devices such as phones or cameras connect and execute different operations without your knowledge.

      ❍ **Critical Windows updates**
      A list of critical Windows updates that are not installed on your computer is displayed. A system restart may be required to allow Bitdefender finish the installation. Please note that it may take a while to install the updates.

      ❍ **Weak Windows accounts**

You can see the list of the Windows user accounts configured on your device and the level of protection their password provides. You can choose between asking the user to change the password at the next login or changing the password yourself immediately. To set a new password for your system, select **Change the password now**.

To create a strong password, we recommend you to use a combination of uppercase and lowercase letters, numbers and special characters (such as #, $ or @).

❍ **APPLICATIONS**

❍ **Browser Security**

Change upon your device's settings that allows the execution of files and programs downloaded via Internet Explorer without an integrity validation, which may lead to your device being compromised.

❍ **Application updates**

To see information about the app that needs to be updated, click its name from the list.

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

❍ **NETWORK**

❍ **Network and Credentials**

Altered system settings such as automatically connecting to open hotspot networks without your knowledge or not enforcing encryption on the outgoing secure channel traffic.

❍ **Wi-Fi networks and routers**

To find out more about the wireless network and router you are connected to, click its name from the list. If it is recommended to set a stronger password for your home network, make sure that you follow our instructions, so that you can stay connected without worrying about your privacy.

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

Using automatic vulnerability monitoring

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

To check and fix the detected issues:

1. Click **Notifications** on the navigation menu on the Bitdefender interface.
2. In the **All** tab, select the notification regarding the Vulnerability scan.
3. You can see detailed information regarding the detected system vulnerabilities. Depending on the issue, to fix a specific vulnerability proceed as follows:

   ❍ If Windows updates are available, click **Install**.

   ❍ If automatic Windows update is disabled, click **Enable**.

   ❍ If an app is outdated, click **Update now** to find a link to the vendor webpage from where you can install the latest version of that app.

   ❍ If a Windows user account has a weak password, click **Change password** to force the user to change the password at the next logon or change the password yourself. For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, $ or @).

   ❍ If the Windows Autorun feature is enabled, click **Fix** to disable it.

   ❍ If the router you have configured has set a weak password, click **Change password** to access its interface from where you can set a strong one.

   ❍ If the network you are connected to has vulnerabilities which may expose your system at risk, click **Change Wi-Fi settings**.

To configure the vulnerability monitoring settings:

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

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

3. Go to the **Settings** tab.

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

Windows updates

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

Application updates

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

User passwords

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

Autoplay

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

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

Wi-Fi Security Advisor

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

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

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

Wi-Fi Security Advisor

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

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

Usually, public wireless networks are more likely to be unsafe since they do not require password at login, and if they do, the password could be made available to anybody who wants to connect. Moreover, they may be malicious or honeypot networks, representing a target for cyber criminals.

The Bitdefender Wi-Fi Security Advisor gives information about:

❍ Home Wi-Fi networks

❍ Office Wi-Fi networks

❍ Public Wi-Fi networks

Turning on or off Wi-Fi Security Advisor notifications

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

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

2. In the **VULNERABILITY** pane, click **Open**.

3. Go to the **Settings** window and turn on or off the **Wi-Fi Security Advisor** option.

Configuring Home Wi-Fi network

To start configuring your home network:

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

2. In the **VULNERABILITY** pane, click **Open**.

3. Go to the **Wi-Fi Security Advisor** window and click **Home Wi-Fi**.

4. In the **Home Wi-Fi** tab, click **SELECT HOME WI-FI**.

A list with the wireless networks you connected to until now is displayed.

5. Point to your home network, and then click **SELECT**.

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

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

To add a new wireless network as home, click **Select new home wi-fi**.

Configuring Office Wi-Fi network

To start configuring your office network:

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

2. In the **VULNERABILITY** pane, click **Open**.

3. Go to the **Wi-Fi Security Advisor** window, click **Office Wi-Fi**.

4. In the **Office Wi-Fi** tab, click **SELECT OFFICE WI-FI**.
   A list with the wireless networks you connected to until now is displayed.

5. Point to your office network, and then click **SELECT**.

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

To remove the wireless network you have set as office network, click **REMOVE**.

To add a new wireless network as office, click **Select new office wi-fi**.

Public Wi-Fi

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

❍ Advanced Threat Defense is turned on

❍ The Bitdefender Firewall is turned on and the following settings are applied to your wireless adapter:

❍ Stealth mode - ON

❍ Network type - Public

❍ The following settings from Online Threat Prevention are turned on:

❍ Encrypted web scan

❍ Protection against fraud

❍ Protection against phishing

❍ A button that opens Bitdefender Safepay™ is available. In this case, the Hotspot protection for unsecured networks is enabled by default.

Checking information about Wi-Fi networks

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

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

2. In the **VULNERABILITY** pane, click **Open**.

3. Go to the **Wi-Fi Security Advisor** window.

4. Depending on the information you need, select one of the three tabs, **Home Wi-Fi**, **Office Wi-Fi** or **Public Wi-Fi**.

5. Click **View details** next to the network you want to find more info about.

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

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

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

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

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

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

❍ **Encryption type** - here you can view the encryption type used by the selected network. Some encryption types may not be secure. Therefore, we strongly recommend you to check information about the displayed encryption type to be sure that you are protected while surfing the web.

❍ **Channel/Frequency** - here you can view the channel frequency used by the selected network.

❍ **Password strength** - here you can view how strong the password is. Note that the networks that have set weak passwords represent a target to cyber criminals.

❍ **Type of sign in** - here you can view if the selected network is protected using a password or not. It is highly recommended to connect only to networks that have set strong passwords.

❍ **Authentication type** - here you can view the authentication type used by the selected network.

3.2.8. Video & Audio Protection

More and more threats are designed to access built-in webcams and microphones. To prevent unauthorized access to your webcam and to inform you what unstrusted apps access your device's microphone and when, Bitdefender Video & Audio has included:

❍ Webcam Protection

❍ Microphone Monitor

Webcam Protection

That hackers may take over your webcam to spy on you is not a novelty anymore, and solutions to protect it, such as revoking app's privileges, disable the device's built-in camera, or to cover it up are not very practical. To prevent further attempts to gain access to your privacy, Bitdefender

Webcam Protection permanently monitors the apps that try to get access to your camera and blocks those that are not listed as trusted.

As a safety measure you will be notified each time an untrusted app will attempt to gain access to your camera.

Turning on or off Webcam Protection

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

2. In the **VIDEO & AUDIO PROTECTION** pane, click **Settings**.

3. Now go to the **Settings** window and turn on or off the corresponding switch.

Configuring Webcam Protection

You can configure which rules should be applied when an app will try to gain access to your camera by following these steps:

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

2. In the **VIDEO & AUDIO PROTECTION** pane, click **Settings**.

3. Go to the **Settings** tab.

The following options are available:

Application block rules

❍ **Block all access to the webcam** - no app will be allowed to gain access to your webcam.

❍ **Block browsers' access to the webcam** - no web browser except Internet Explorer and Microsoft Edge will be allowed to gain access to your webcam. Due to the Windows Store apps procedure to run in a single process, Internet Explorer and Microsoft Edge cannot be detected by Bitdefender as web browsers, and therefore are excepted from this setting.

❍ **Set application permissions based on community choice** - if the majority of Bitdefender users consider a popular app as being harmless, then its access to the webcam will be automatically set on Allow. If a popular app is considered as dangerous by the many, then its access will be automatically set on Blocked.

Notifications

❍ **Notify when allowed applications connect to the webcam** - you will be notified each time an allowed app will access your webcam.

Adding apps to the Webcam Protection list

Apps that try to connect to your webcam are automatically detected and depending on their behavior and the community's choice, their access is allowed or denied. However, you can manually start configuring on your own what action should be taken by following these steps:

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

2. In the **VIDEO & AUDIO PROTECTION** pane, click **Settings**.

3. Go to the **Webcam Protection** window.

4. Click **Add application** window.

5. Click the desired link:

❍ **From Windows Store** - a list with the detected Windows Store apps is displayed. Turn on the switches next to the apps you want to add to the list.

❍ **From your apps** - go to the .exe file you want to add to the list, and then click **OK**.

To view what the Bitdefender users have chosen to do with the selected app, click the ⬈ icon.

The apps that will request access to your camera together with the time of last activity will appear in this window.

You will be notified each time one of the allowed apps is blocked by the Bitdefender users.

To stop the access of an added app to your webcam, click the 🎥 icon.

The icon turns to 🚫, meaning that the selected app will have no access to your webcam.

Microphone monitor

Rogue apps may access your built-in microphone silently or in the background without your consent. To make you aware of potential malicious exploits, Bitdefender Microphone monitor will give you notice of such events. This way, no app will be able to gain access to your microphone without you being in charge.

Turning on or off Microphone monitor

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

2. In the **VIDEO & AUDIO PROTECTION** pane, click **Settings**.

3. Select the **Settings** window.

4. In the **Settings** window, turn on or off the **Microphone monitor** switch.

Configuring notifications for Microphone monitor

To configure what notifications should appear when apps will try to gain access to your microphone, follow these steps:

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

2. In the **VIDEO & AUDIO PROTECTION** pane, click **Settings**.

3. Go to the **Settings** window.

Notifications

❍ **Notify when an application tries to access the microphone**

❍ **Notify when browsers access the microphone**

❍ **Notify when untrusted apps access the microphone**

❍ **Display notification based on Bitdefender users' choice**

Adding apps to the Microphone monitor list

Apps that will try to connect to your microphone will be automatically detected and added to the Notification list. However, you can manually configure on your own if a notification should be displayed or not by following these steps:

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

2. In the **VIDEO & AUDIO PROTECTION** pane, click **Settings**.

3. Go to the **Audio Protection** window.

4. Click **Add application** window.

5. Click the desired link:

❍ **From Windows Store** - a list with the detected Windows Store apps is displayed. Turn on the switches next to the apps you want to add to the list.

❍ **From your apps** - go to the .exe file you want to add to the list, and then click **OK**.

To view what the Bitdefender users have chosen to do with the selected app, click the ⬈ icon.

The apps that will request access to your microphone together with the time of last activity will appear in this window.

To stop receiving notifications regarding the activity of an added app, click the 🎤 icon.

The icon turns to 🎤̸ , meaning that no Bitdefender notification will be displayed when the selected app will try to access your microphone.

3.2.9. Ransomware Remediation

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

Turning on or off Ransomware Remediation

To turn on or off Ransomware Remediation:

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

2. In the **RANSOMWARE REMEDIATION** pane, turn on or off the switch.

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

Turning on or off automatic restore

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

To turn on or off automatic restore:

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

2. In the **RANSOMWARE REMEDIATION** pane, click **Manage**.

3. In the Settings window, turn on or off the **Automatic restore** switch.

Viewing files that were automatically restored

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

To view files that were automatically restored:

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

2. In the **All** tab, select the notification regarding the latest ransomware behavior remediated, and then click **Restored Files**.
The list with the restored files is displayed. Here you can also view the location where your files have been restored.

Restoring encrypted files manually

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

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

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

3. The list with the encrypted files is displayed.
Click **Recover Files** to continue.

4. In case the entire or a part of the restoring process fails, you have to choose the location where the decrypted files should be saved. Click **Restore location**, and then choose a location on your PC.

5. A confirmation window appears.
Click **Finish** to end the restoring process.

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

.3g2;.3gp;.7z;.ai;.aif;.arj;.asp;.aspx;.avi;.bat;.bin;.bmp;.c;.cda;.cgi;.class;.com;.cpp;.cs;.css;.csv;.dat;.db;.dbf;.deb;.doc;.docx;.gif;.gz;.h264;.h;.flv;.ht

m;.html;.ico;.jar;.java;.jpeg;.jpg;.js;.jsp;.key;.m4v;.mdb;.mid;.midi;.mkv;.m
p3;.mp4;.mov;.mpg;.mpeg;.ods;.odp;.odt;.ogg;.pdf;.pkg;.php;.pl;.png;.pps;
.ppt;.pptx;.ps;.psd;.py;.rar;.rm;.rtf;.sav;.sql;.sh;.svg;.swift;.swf;.tar;.tex;.tif;
.tiff;.txt;.xlr;.xls;.xlsx;.xml;.wmv;.vb;.vob;.wav;.wks;.wma;.wpl;.wps;.wpd;.
wsf;.z;.zip;

Adding applications to exceptions

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

To add apps to the Ransomware Remediation exceptions list:

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

2. In the **RANSOMWARE REMEDIATION** pane, click **Manage**.

3. Go to the **Exceptions** window and click **+Add an Exception**.

3.2.10. Cryptomining Protection

What is Cryptomining Protection?

With the use of cryptomining attackers can benefit financially without carrying the assosiated costs and legal consequences.

Bitdefender's Cryptomining Protection feature defends Windows computers against the growing threat of unauthorized crypto-mining activities, a malicious practice that exploits a user's resources and electricity to generate revenue for attackers.

> ℹ️ Note
> Cryptomining Protection relies on:
>
> ❍ Bitdefender Shield
>
> ❍ Web Attack Prevention
>
> In order to have Cryptomining Protection capable of running, both of these two features must be enabled as well.

Enabling Cryptomining Protection

The Cryptomining Protection feature is located within the Protection tab.

To enable it, simply toggle its corresponding switch.

> **i** Note
> Cryptomining Protection is disabled by default, ensuring that users have control over its activation.

Modes of operation

Once enabled, the Cryptomining Protection feature operates in 2 distinct states, each tailored to the user's preferences:

1. **Block all Cryptomining activities.** (automatically blocks any crypto-mining activities and takes necessary actions to prevent further unauthorized attempts)

   This mode is ideal for users who have no intention of engaging in crypto-mining activities.

2. **Detect Cryptomining activities.** (issues alerts whenever a crypto-mining activity is detected and requires user input to determine the appropriate action)

   This mode is suited for users actively involved in their own crypto-mining activities but wish to monitor and control any unauthorized attempts.

Manage exceptions

Exceptions can be specified for applications, with the added capability of defining specific command lines. However, exceptions can also be established without the need for providing such detailed parameters, offering a balance between customization and simplicity.

To add an exception:

1. Click **Protection** on the left-hand side menu on the Bitdefender interface.

2. In the **Cryptomining Protection** pane, click **Settings**.

3. Click the **Manage exceptions** option.

4. Next, click the **Add an Exception** button.

5. A new window will open. You can manually exclude applications, URLs, and IP addresses.

6. Finally, click **Save**. The new rule is added to Cryptomining Protection exceptions list.

> **i** Note
> To remove an exception, simply click the trash can icon next to it.

3.2.11. Scam Copilot for Windows

Scam Copilot is Bitdefender's AI-powered scam detector.

In using it, you can send any tricky texts, emails, social media messages, links or even QR codes you've received and are suspicious of, in order to get an instant analysis on their safety and legitimacy.

To set up Scam Copilot:

1. Open Bitdefender.
2. Open the Protection tab in the left side menu of the Bitdefender window.
3. Click on the **Get started** button.
4. From here, follow all on-screen instructions to enable all components of the Scam Copilot module.

Scam Copilot will then successfully be setup on your device!

In the Scam Copilot dashboard, you are able to see the amount of verified and detected messages, emails and links you are receiving and which are continousely monitored by Bitdefender, as well as the number of potential scams checked and detected so far.

In the same dashboard, you also have the option to chat with Scam Copilot, when you feel as though you might be targeted by a scam or phishing attempt.

3.2.12. 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:

❍ Internet Explorer

❍ Google Chrome

❍ Mozilla Firefox

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.

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.

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.

❍ From the Bitdefender interface:

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

2. In the **ANTI-TRACKER** pane, click **Settings**.

3. Next to the web browser for which you want to disable the extension, turn off the corresponding switch.

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 ⊕ .

3.2.13. Safepay security for online transactions

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

This involves sending personal information, account and credit card data, passwords and other types of private information over the internet, in other words exactly the type of information flow that cyber-criminals are very interested to tap into. Hackers are relentless in their efforts to steal

this information, so you can never be too careful about securing online transactions.

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

Bitdefender Safepay™ offers the following features:

❍ It blocks access to your desktop and any attempt to take snapshots of your screen.

❍ It comes with a virtual keyboard which, when used, makes it impossible for hackers to read your keystrokes.

❍ It is completely independent from your other browsers.

❍ It comes with built-in hotspot protection to be used when your device is connected to unsecured Wi-fi networks.

❍ It supports bookmarks and allows you to navigate between your favorite banking/shopping sites.

❍ It is not limited to banking and e-shopping. Any website can be opened in Bitdefender Safepay™.

Using Bitdefender Safepay™

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

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

❍ From the Bitdefender interface:

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

2. In the **SAFEPAY** pane, click **Settings**.

3. In the **Safepay** window, click **Launch Safepay**.

❍ From Windows:

❍ In **Windows 7**:

1. Click **Start** and go to **All Programs**.

2. Click **Bitdefender**.

3. Click **Bitdefender Safepay™**.

❍ In **Windows 8.1**:
Locate Bitdefender Safepay™ from the Windows Start screen (for example, you can start typing "Bitdefender Safepay™" directly in the Start screen) and then click the icon.

❍ In **Windows 10** and **Windows 11**:
Type "Bitdefender Safepay™" in the search box from the taskbar and click its icon.

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

❍ enter URLs you want to go to in the address bar.

❍ add tabs to visit multiple websites in the Bitdefender Safepay™ window by clicking ➕ .

❍ navigate back and forward and refresh pages using ← → ↻ respectively.

❍ access Bitdefender Safepay™ settings by clicking and choosing **Settings**.

❍ manage your bookmarks by clicking ☆ next to the address bar.

❍ open the virtual keyboard by clicking ⊕ .

❍ increase or decrease the browser size by pressing simultaneously **Ctrl** and the **+/-** keys in the numeric keypad.

❍ view information about your Bitdefender product by clicking ⋯ and choosing **About**.

❍ print important information by clicking ⋯ and choosing **Print**.

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

Configuring settings

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

Apply Bitdefender Safepay rules for accessed domains

The websites you have added to Bookmarks with the **Automatically open in Safepay** option enabled will appear here. If you want to stop automatically opening with Bitdefender Safepay™ a website from the list, click × next to the desired entry from the **Remove** column.

Block pop-ups

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

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

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

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

Manage Plugins

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

Manage certificates

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

Click **IMPORT** and follow the wizard to use the certificates in Bitdefender Safepay™.

Use Virtual Keyboard

The Virtual Keyboard will automatically appear when a password field is selected.

Use the corresponding switch to enable or disable the feature.

Printing confirmation

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

Managing bookmarks

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

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

1. Click ⋯ and choose **Bookmarks** to open the Bookmarks page.

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

2. Click the **+** button to add a new bookmark.

3. Type the URL and the title of the bookmark, and then click **CREATE**. Check the **Automatically open in Safepay** option if you want the bookmarked page to open with Bitdefender Safepay™ each time you access it. The URL is also added to the Domains list on the settings page.

Turning off Safepay notifications

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

To turn off the Safepay notifications:

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

2. In the **SAFEPAY** pane, click **Settings**.

3. In the **Settings** window, turn off the switch next to **Safepay notifications**.

3.2.14. Device Anti-Theft

Laptop theft is a major issue that affects individuals and organizations alike. Even more than losing the hardware itself, the data lost with it can cause significant damage, both financially and emotionally.

Yet few people take the proper steps to secure their important personal, business and financial data in the case of theft or loss.

Bitdefender Anti-Theft helps you be better prepared for such an event by allowing you to remotely locate or lock your laptop and even wipe all data from it, should you ever part with your laptop against your will.

To use the Anti-Theft features, the following prerequisites must be met:

❍ The commands can only be sent from the Bitdefender account.

❍ The laptop must be connected to the internet to receive the commands.

Anti-Theft features work in the following way:

Locate

View your device's location on Google Maps.

The accuracy of the location depends on how Bitdefender is able to determine it. The location is determined to within tens of meters if Wi-fi is enabled on your laptop and there are wireless networks in its range.

If the laptop is connected to a wired LAN with no Wi-fi based location available, the location will be determined based on the IP address, which is considerably less accurate.

Alert

Send a remote alert on the device.

The feature is only available on mobile devices.

Lock

Lock your laptop and set a 4 digit PIN for unlocking it. When you send the **Lock** command, the system reboots and logging back into Windows is only possible after entering the PIN you have set.

If you want Bitdefender to take photos of the one who tries to get access to your laptop, check the corresponding check box. The snapped photos are taken using the front camera and displayed together with the time-stamp in the Anti-Theft dashboard. Only the two most recent photos will be saved.

This action is available only for laptops that have front camera.

Wipe

Remove all data from your system. When you send the **Wipe** command, the laptop reboots and the data on all hard drive partitions is erased.

Show IP

Displays the last IP address for the selected device. Click **SHOW IP** to make it visible.

Anti-Theft is activated after the installation and can be accessed exclusively through your Bitdefender account from any device connected to the internet, anywhere.

Using Anti-Theft features

To access the Anti-Theft features, use one of the following possibilities:

❍ From the Bitdefender main interface:

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

2. Click **GO TO CENTRAL**.
   You are redirected to the Bitdefender Central page. Make sure that you are signed in with your credentials.

3. In the Bitdefender Central window that opens, click the desired device card, then select **Anti-Theft**.

❍ On any device with internet access:

1. Open a web browser and go to: https://central.bitdefender.com.

2. Sign in to your Bitdefender account using your email address and password.

3. Select the **My Devices** panel.

4. Click the desired device card, then select **Anti-Theft**.

5. Select the feature you want to use:
   Locate - display your device's location on Google Maps.
   Show IP - display the last IP address of your device.
   📶 **Alert** - send an alert on the device.
   🔒 **Lock** - lock your laptop and set a PIN code for unlocking it.
   🗑 **Wipe** - delete all data from your laptop.

> ! **Important**
> After you wipe a device, all Anti-Theft features cease to function.

3.3. Utilities

3.3.1. Profiles

Daily job activities, watching movies or playing games may cause system slow down, especially if they are running simultaneously with Windows update processes and maintenance tasks. With Bitdefender, you can now

choose and apply your preferred profile, which makes system adjustments suited to increase the performance of specific installed apps.

Bitdefender provides the following profiles:

❍ Work Profile

❍ Movie Profile

❍ Game Profile

❍ Public Wi-Fi Profile

❍ Battery Mode Profile

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

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

❍ All Bitdefender alerts and pop-ups are disabled.

❍ Automatic Update is postponed.

❍ Scheduled scans are postponed.

❍ The Antispam feature is enabled.

❍ Search Advisor is disabled.

❍ Special offers notifications are disabled.

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

❍ Windows Automatic Updates are postponed.

❍ Windows alerts and pop-ups are disabled.

❍ Unnecessary background programs are suspended.

❍ Visual effects are adjusted for best performance.

❍ Maintenance tasks are postponed.

❍ Power plan settings are adjusted.

While running in the Public Wi-Fi profile, Bitdefender Ultimate Small Business Security is set to automatically accomplish the following program settings:

❍ Advanced Threat Defense is turned on

❍ The Bitdefender Firewall is turned on and the following settings are applied to your wireless adapter:

  ❍ Stealth mode - ON

  ❍ Network type - Public

❍ The following settings from Online Threat Prevention are turned on:

  ❍ Encrypted web scan

  ❍ Protection against fraud

  ❍ Protection against phishing

Work Profile

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

Configuring Work Profile

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

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

2. In the **Profiles** tab, click **Settings**.

3. Click the **CONFIGURE** button from the Work Profile area.

4. Choose the system adjustments you would like to be applied by checking the following options:

  ❍ Boost performance on work apps

  ❍ Optimize product settings for Work profile

  ❍ Postpone background programs and maintenance tasks

  ❍ Postpone Windows Automatic Updates

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

Manually adding apps to the Work Profile list

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

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

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

2. In the **Profiles** tab, click **Settings**.

3. Click the **CONFIGURE** button from the Work Profile area.

4. In the **Work profile settings** window, click **Applications list**.

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

Movie Profile

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

Configuring Movie Profile

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

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

2. In the **Profiles** tab, click **Settings**.

3. Click the **CONFIGURE** button from the Movie Profile area.

4. Choose the system adjustments you would like to be applied by checking the following options:

   ❍ Boost performance on video players

   ❍ Optimize product settings for Movie profile

   ❍ Postpone background programs and maintenance tasks

   ❍ Postpone Windows Automatic Updates

   ❍ Adjust power plan settings for movies

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

Manually adding video players to the Movie Profile list

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

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

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

2. In the **Profiles** tab, click **Settings**.

3. Click the **CONFIGURE** button from the Movie Profile area.

4. In the **Movie profile settings** window, click **Players list**.

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

Game Profile

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

Configuring Game Profile

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

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

2. In the **Profiles** tab, click **Settings**.

3. Click the **Configure** button from the Game Profile area.

4. Choose the system adjustments you would like to be applied by checking the following options:

   ❍ Boost performance on games

   ❍ Optimize product settings for Game profile

   ❍ Postpone background programs and maintenance tasks

❍ Postpone Windows Automatic Updates

❍ Adjust power plan settings for games

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

Manually adding games to the Game list

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

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

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

2. In the **Profiles** tab, click **Settings**.

3. Click the **Configure** button from the Game Profile area.

4. In the **Game profile settings** window, click **Games list**.

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

Public Wi-Fi Profile

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

Configuring Public Wi-Fi profile

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

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

2. In the **Profiles** tab, click **Settings**.

3. Click the **CONFIGURE** button from the Public Wi-Fi Profile area.

4. Let the **Adjusts product settings to boost protection when connected to an unsafe public Wi-Fi network** check box enabled.

5. Click **Save**.

Battery Mode Profile

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

Configuring Battery Mode Profile

To configure the Battery Mode profile:

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

2. In the **Profiles** tab, click **Settings**.

3. Click the **Configure** button from the Battery Mode Profile area.

4. Choose the system adjustments to be applied by checking the following options:

   ❍ Optimize product settings for Battery mode.

   ❍ Postpone background programs and maintenance tasks.

   ❍ Postpone Windows Automatic Updates.

   ❍ Adjust power plan settings for Battery mode.

   ❍ Disable external devices and network ports.

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

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

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

❍ Bitdefender Automatic Update is postponed.

❍ Scheduled scans are postponed.

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

Real-time optimization

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

To turn on or off Real-time optimization:

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

2. In the **Profiles** tab, click **Settings**.

3. Scroll down until you see the Real-time optimization option, and then use the corresponding switch to turn it on or off.

3.3.2. OneClick Optimizer

Issues such as hard disk failures, leftover registry files and browser history, may slow down your work, which may become nagging for you. All these can now be fixed with one single click of a button.

OneClick Optimizer allows you to identify and remove useless files by running multiple cleaning tasks at the same time.

To start the OneClick Optimizer process:

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

2. Click the **Optimize** button.

   a. **Analyzing**
   Wait for Bitdefender to finish searching for system issues.

   ❍ Disk Cleanup - identifies unnecessary files and folders.

   ❍ Registry Cleanup - identifies invalid or outdated references in the Windows Registry.

   ❍ Privacy Cleanup - identifies temporary internet files and cookies, browser cache and history.

   The number of found issues is displayed. Click the View details link to review them before proceeding with the cleaning process. Click Optimize to continue.

   b. **Optimizing**

Wait for Bitdefender to finish optimizing your system.

c. **Issues**

This is where you can view the operation result.

If you want comprehensive information on the optimization process, click the **View detailed report** button.

3.3.3. Data Protection

Deleting files permanently

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

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

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

1. Right-click the file or folder you want to permanently delete.

2. Select **Bitdefender > File Shredder** in the context menu that appears.

3. Click **Delete permanently**, and then confirm that you wish to continue with the process.
   Wait for Bitdefender to finish shredding the files.

4. The results are displayed. Click **Finish** to exit the wizard.

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

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

2. In the **Data Protection** pane, click **File Shredder**.

3. Follow the File Shredder wizard:

   a. Click the **Add Folders** button to add the files or folders you want to be permanently removed.
      Alternatively, drag these files or folders to this window.

   b. Click **Delete Permanently**, and then confirm that you wish to continue with the process.
      Wait for Bitdefender to finish shredding the files.

c. **Results Summary**
The results are displayed. Click **Finish** to exit the wizard.

3.4. How to

3.4.1. Installation

How do I install Bitdefender on a second device?

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

To install Bitdefender on a second device:

1. Click **Install on another device** on the lower-left corner of the Bitdefender interface.
   A new window appears on your screen.

2. Click **SHARE DOWNLOAD LINK**.

3. Follow the on-screen instructions to install Bitdefender.

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

How can I reinstall Bitdefender?

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

❍ you have reinstalled the operating system.

❍ you want to fix issues that might have caused slowdowns and crashes.

❍ your Bitdefender product is not starting or working properly.

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

❍ In **Windows 7**:

1. Click **Start** and go to **All Programs**.

2. Find **Bitdefender Ultimate Small Business Security** and select **Uninstall**.

3. Click **REINSTALL** in the window that appears.

4. You need to restart the device to complete the process.

❍ In **Windows 8.1**:

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 Ultimate Small Business Security** and select **Uninstall**.

4. Click **REINSTALL** in the window that appears.

5. You need to restart the device to complete the process.

❍ In **Windows 10** and **Windows 11**:

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

2. Click the **System** icon in the Settings area, then select **Apps & features**.

3. Find **Bitdefender Ultimate Small Business Security** and select **Uninstall**.

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

5. Click **REINSTALL**.

6. You need to restart the device to complete the process.

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

Where can I download my Bitdefender product from?

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

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

To install Bitdefender from Bitdefender Central:

1. Access Bitdefender Central.

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

3. Choose one of the two available options:

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

   ❍ **Protect other devices**
   Select this option, and then select the owner of the device. If the device belongs to someone else, click the corresponding button.
   Click **SEND DOWNLOAD LINK**. Type an email address in the corresponding field, and click **SEND EMAIL**. Note that the generated download link is valid for the next 24 hours only. If the link expires, you will have to generate a new one by following the same steps.
   On the device you want to install your Bitdefender product, check the email account that you typed in, and then click the corresponding download button.

4. Run the Bitdefender product you have downloaded.

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

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

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

❍ From a previous Bitdefender Antivirus version to the latest Bitdefender Antivirus available.

❍ From a previous Bitdefender Internet Security version to the latest Bitdefender Internet Security available.

❍ From a previous Bitdefender Total Security version to the latest Bitdefender Total Security available.

There are two cases which may appear:

❍ You have upgraded the operating system using Windows Update and you notice Bitdefender is no longer working.
In this case, you need to reinstall the product by following these steps:

❍ In **Windows 7**:

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

2. Find **Bitdefender Ultimate Small Business Security** and select **Uninstall**.

3. Click **REINSTALL** in the window that appears.

4. Wait for the uninstall process to complete, and then reboot your system.
Open the interface of your new installed Bitdefender product to have access to its features.

❍ In **Windows 8.1**:

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 Ultimate Small Business Security** and select **Uninstall**.

4. Click **REINSTALL** in the window that appears.

5. Wait for the uninstall process to complete, and then reboot your system.
Open the interface of your new installed Bitdefender product to have access to its features.

❍ In **Windows 10** and **Windows 11**:

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

2. Click the **System** icon in the Settings area, then select **Apps**.

3. Find **Bitdefender Ultimate Small Business Security** and select **Uninstall**.

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

5. Click **REINSTALL** in the window that appears.

6. Wait for the uninstall process to complete, and then reboot your system.
   Open the interface of your new installed Bitdefender product to have access to its features.

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

❍ You changed your system and you want to continue using the Bitdefender protection. Therefore, you need to reinstall the product using the latest version.
To solve this situation:

1. Download the installation file:

   a. Access Bitdefender Central.

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

   c. Choose one of the two available options:

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

      ❍ **Protect another device**
      Select this option, and then select the owner of the device. If the device belongs to someone else, click the corresponding button.
      Click **SEND DOWNLOAD LINK**. Type an email address in the corresponding field, and click **SEND EMAIL**. Note that the generated download link is valid for the next 24 hours only. If the link expires, you will have to generate a new one by following the same steps.
      On the device you want to install your Bitdefender product, check the email account that you typed in, and then click the corresponding download button.

2. Run the Bitdefender product you have downloaded.

For more information about the Bitdefender installation process, refer to Installing your Bitdefender product (page 11).

How can I upgrade to the latest Bitdefender version?

From now on, the upgrade to the newest version is possible without following the manual uninstall and reinstall procedure. More exactly, the new product including new features and major product improvements is delivered via product update and, if you already have an active Bitdefender subscription, the product gets automatically activated.

If you are using the 2020 version, you can upgrade to the newest version by following these steps:

1. Click **RESTART NOW** in the notification you receive with the upgrade information. If you miss it, access the Notifications window, point to the most recent update, and then click the **RESTART NOW** button. Wait for the device to restart.
   The **What's new** window with information about the improved and new features appears.

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

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

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

3.4.2. Bitdefender Central

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

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

To successfully sign in with another Bitdefender account:

1. Click on your account name in the upper part of the Bitdefender interface.

2. Click **Switch Account** on the upper right corner of the screen to change the account linked to the device.

3. Type the email address in the corresponding field, and then click **NEXT**.

4. Type your password, and then click **SIGN IN**.

> **ⓘ Note**
> The Bitdefender product from your device automatically changes according to the subscription associated to the new Bitdefender account. If there is no available subscription associated to the new Bitdefender account, or you wish to transfer it from the previous account, you can contact Bitdefender for support as described in section Asking for Help (page 270).

How do I turn off Bitdefender Central help messages?

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

If you wish to stop seeing this kind of messages:

1. Access Bitdefender Central.

2. Click the ⦁ icon in the upper right side of the screen.

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

4. Click **Settings** in the slide menu.

5. Disable the Turn **on/off help messages** option.

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

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

❍ From the Bitdefender interface:

1. Click **My Account** on the navigation menu on the Bitdefender interface.

2. Click **Switch Account** on the upper right corner of the screen.

A new window appears.

3. Type your email address and click **NEXT**.
A new window appears.

4. Click **Forgot password?**.

5. Click **NEXT**.

6. Check your email account, type the security code you have received, and then click **NEXT**.
Alternatively, you can click **Change password** in the email that we sent you.

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

❍ From your web browser:

1. Go to: https://central.bitdefender.com.

2. Click **SIGN IN**.

3. Type your email address, and then click **NEXT**.

4. Click **Forgot password?**.

5. Click **NEXT**.

6. Check your email account and follow the provided instructions to set a new password for your Bitdefender account.

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

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

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

1. Access Bitdefender Central.

2. Click the ⋏ icon in the upper right side of the screen.

3. Click **Sessions** in the slide menu.

4. In the **Active sessions** area, select the **SIGN OUT** option next to the device you want to finish the logon session.

3.4.3. Scanning with Bitdefender

How do I scan a file or a folder?

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

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

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

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

❍ You suspect a specific file or folder to be infected.

❍ Whenever you download files from the internet that you think might be dangerous.

❍ Scan a network share before copying files to your device.

How do I scan my system

To perform a complete scan on the system:

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. Click the **Run Scan** button next to **System Scan**.

4. Follow the System Scan wizard to complete the scan. Bitdefender will automatically take the recommended actions on detected files.
   If there remain unresolved threats, you will be prompted to choose the actions to be taken on them. For more information, refer to.

How do I schedule a scan?

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

To schedule a scan:

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. Click ⋯ next to the scan type that you want to schedule, System Scan or Quick Scan, in the lower part of the interface, then select **Edit**. Alternatively, you can create a scan type to suit your needs by clicking **+Create Scan** next to **Manage Scans**.

4. Customize the scan according to your needs, then click **Next**.

5. Check the box next to **Choose when to schedule this task**.
   Select one of the corresponding options to set a schedule:

   ❍ At system startup

   ❍ Daily

   ❍ Weekly

   ❍ Monthly

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

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

How do I create a custom scan task?

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

To create a customized scan task, proceed as follows:

1. In the **ANTIVIRUS** pane, click **Open**.

2. Click **+Create Scan** next to **Manage Scans**.

3. In the task name field, type a name for the scan, select the locations you would like to be scanned, and then click **NEXT**.

4. Configure these general options:

   ❍ **Scan only applications**. You can set Bitdefender to scan only accessed apps.

   ❍ **Scan task priority**. You can choose the impact a scan process should have on your system performance.

❍ Auto - The priority of the scan process will depend on the system activity. To make sure that the scan process will not affect the system activity, Bitdefender will decide whether the scan process should be run with high or low priority.

❍ High - The priority of the scan process will be high. By choosing this option, you will allow other programs to run slower and decrease the time needed for the scan process to finish.

❍ Low - The priority of the scan process will be low. By choosing this option, you will allow other programs to run faster and increase the time needed for the scan process to finish.

❍ **Post scan actions**. Choose what action Bitdefender should take in case no threats are found:

❍ Show Summary window

❍ Shutdown device

❍ Close Scan window

5. If you want to configure the scanning options in detail, click **Show advanced options**.
   Click **Next**.

6. You can enable the **Schedule scan task** option, if you wish, then choose when the custom scan you created should start.

❍ At system startup

❍ Daily

❍ Monthly

❍ Weekly

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

7. Click **Save** to save the settings and close the configuration window.
   Depending on the locations to be scanned, the scan may take a while. If threats will be found during the scanning process, you will be prompted to choose the actions to be taken on the detected files.

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

How do I except a folder from being scanned?

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

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

❍ You have a large folder on your system where you keep movies and music.

❍ You have a large archive on your system where you keep different data.

❍ You keep a folder where you install different types of software and apps for testing purposes. Scanning the folder may result in losing some of the data.

To add a folder to the Exceptions list:

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. Click the **Settings** tab.

4. Click on **Manage Exceptions**.

5. Click **+Add an Exception**.

6. Enter the path of the folder you want to except from scanning in the corresponding field.
   Alternatively, you can navigate to the folder by clicking the browse button in the right side of the interface, select it and click on **OK**.

7. Turn on the switch next to the protection feature that should not scan the folder. There are three options:

   ❍ Antivirus

   ❍ Online Threat Prevention

   ❍ Advanced Threat Defense

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

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

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

1. Turn off the Bitdefender real-time antivirus protection:

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

   b. In the **ANTIVIRUS** pane, click **Open**.

   c. In the **Advanced** window, turn off **Bitdefender Shield**.
   A warning window appears. You must confirm your choice by selecting from the menu how long you want the real-time protection to be disabled. You can disable real-time protection for 5, 15 or 30 minutes, for an hour, permanently or until a system restart.

2. Display hidden objects in Windows. To find out how to do this, refer to How do I display hidden objects in Windows? (page 112).

3. Restore the file from the Quarantine area:

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

   b. In the **ANTIVIRUS** pane, click **Open**.

   c. Go to the **Settings** windows and click **Manage quarantine**.

   d. Select the file, and then click **Restore**.

4. Add the file to the Exceptions list. To find out how to do this, refer to How do I except a folder from being scanned? (page 100).

5. Turn on the Bitdefender real-time antivirus protection.

6. Contact our support representatives so that we may remove the detection of the threat information update. To find out how to do this, refer to Asking for Help (page 270).

How do I check what threats Bitdefender detected?

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

The scan log contains detailed information about the logged scanning process, such as scanning options, the scanning target, the threats found and the actions taken on these threats.

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

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

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

2. In the **All** tab, select the notification regarding the latest scan.
   This is where you can find all threat scan events, including threats detected by on-access scanning, user-initiated scans and status changes for automatic scans.

3. In the notifications list, you can check what scans have been performed recently. Click a notification to view details about it.

4. To open a scan log, click **View log**.

3.4.4. Privacy protection

How do I make sure my online transaction is secure?

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

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

To keep your online activity secure and private:

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

2. In the **SAFEPAY** pane, click **Settings**.

3. In the **Safepay** window, click **Launch Safepay**.

4. Click the ⊕ button to access the **Virtual Keyboard**.
   Use the **Virtual Keyboard** when typing sensitive information such as your passwords.

What can I do if my device has been stolen?

Mobile device theft, whether it is a smartphone, a tablet or a laptop is one of the main issues today affecting individuals and organizations throughout the world.

Bitdefender Anti-Theft allows you to not only locate and lock the stolen device, but also wipe all data to ensure that it will not be used by the thief.

To access the Anti-Theft features from your account:

1. Access Bitdefender Central.

2. Select the **My Devices** panel.

3. Click the desired device card, and then select **Anti-Theft**.

4. Select the feature you want to use:

   ❍ **LOCATE** - display your device's location on Google Maps.
   Show IP - displays the last IP address for the selected device.

   ❍ **Alert** - send an alert on the device.

   ❍ **Lock** - lock your device and set a numeric PIN code for unlocking it. Alternatively, enable the corresponding option to allow Bitdefender to take snapshots of the person who is trying to access your device.

   ❍ **Wipe** - delete all data from your device.

   > **!** **Important**
   > After you wipe a device, all Anti-Theft features cease to function.

How do I remove a file permanently with Bitdefender?

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

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

1. Right-click the file or folder you want to permanently delete, point to Bitdefender and select **File Shredder**.

2. Click **Delete Permanently**, and then confirm that you wish to continue with the process.
   Wait for Bitdefender to finish shredding the files.

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

How do I protect my webcam from being hacked?

You can set your Bitdefender product to allow or deny the access of installed apps to your webcam by following these steps:

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

2. In the **VIDEO & AUDIO PROTECTION** pane, click **Settings**.

3. Go to the **Webcam Protection** window and you will see the list with the apps that have requested access to your camera.

4. Point to the app you want to allow or ban the access, and then click the switch represented by a video camera, situated next to it.
To view what the other Bitdefender users have chosen to do with the selected app, click the ⬈ icon. You will be notified each time one of the listed apps is blocked by the Bitdefender users.

To manually add apps to this list, click the **Add application** button and select one of the two options.

❍ From Windows Store

❍ From your apps

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

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

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

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

3. The list with the encrypted files is displayed.
Click **Recover files** to continue.

4. In case the entire or a part of the restoring process fails, you have to choose the location where the decrypted files should be saved. Click **Restore location**, and then choose a location on your PC.

5. A confirmation window appears.
Click **Finish** to end the restoring process.

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

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

3.4.5. Optimization Tools

How do I improve my system performance?

The system performance depends not only on the hardware configuration, such as the CPU load, memory usage and hard disk space. It is also directly connected to your software configuration and to your data management.

These are the main actions you can take with Bitdefender to improve your system's speed and performance:

❍ Optimize your system performance with a single click (page 105)

❍ Scan your system periodically (page 105)

Optimize your system performance with a single click

The OneClick Optimizer option saves you valuable time when you want a quick way to improve your system performance by rapidly scanning, detecting and cleaning useless files.

To start the OneClick Optimizer process:

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

2. Click the **Optimize** button.

3. Let Bitdefender search for files that can be deleted, then click the **Optimize** button to finish the process.

Scan your system periodically

Your system speed and its general behavior can also be affected by threats.

Make sure to scan your system periodically, at least once a week.

It is recommended to use the System Scan because it scans for all types of threats endangering the security of your system and it also scans inside archives.

To start the System Scan:

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. Click **Run Scan** next to **System Scan**.

4. Follow the wizard steps.

3.4.6. Useful Information

How do I test my security solution?

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

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

To test your security solution:

1. Download the test from the official webpage of the EICAR organization http://www.eicar.org/.

2. Click the **Anti-Malware Testfile** tab.

3. Click **Download** on the left-side menu.

4. From **Download area using the standard protocol http** click the **eicar.com** test file.

5. You will be informed that the page you are trying to access contains the EICAR-Test-File (not a threat).
   If you click **I understand the risks, take me there anyway**, the download of the test will begin and a Bitdefender pop-up will inform you that a threat was detected.
   Click **More details** to find out more information about this action.

If you do not receive any Bitdefender alert, we recommend you to contact Bitdefender for support as described in section Asking for Help (page 270).

How do I remove Bitdefender?

If you want to remove your Bitdefender Ultimate Small Business Security:

❍ In **Windows 7**:

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

2. Find **Bitdefender Ultimate Small Business Security** and select **Uninstall**.

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

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

❍ In **Windows 8.1**:

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 Ultimate Small Business Security** and select **Uninstall**.

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

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

❍ In **Windows 10** and **Windows 11**:

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

2. Click the **System** icon in the Settings area, then select **Apps**.

3. Find **Bitdefender Ultimate Small Business Security** and select **Uninstall**.

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

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

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

> **ⓘ Note**
> This reinstall procedure will permanently delete the customized settings.

How do I remove Bitdefender VPN?

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

❍ 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 8.1**:

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.

How do I remove the Bitdefender Anti-tracker extension?

Depending on the web browser you are using, follow these steps to uninstall the Bitdefender Anti-tracker extension:

❍ Internet Explorer

1. Click ⚙ next to the search bar, and then select Manage add-ons. A list with the installed extensions appears.

2. Click Bitdefender Anti-tracker.

3. Click **Disable** at the bottom right.

❍ Google Chrome

1. Click ⋮ next to the search bar.

2. Select **More Tools**, and then **Extensions**.
A list with the installed extensions appears.

3. Click **Remove** in the Bitdefender Anti-tracker card.

4. Click **Remove** in the popup that appears.

❍ Mozilla Firefox

1. Click ☰ next to the search bar.

2. Select **Add-ons**, and then **Extensions**.
A list with the installed extensions appears.

3. Click ⋯ and then select **Remove**.

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

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

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

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

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

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. In the **Scans** window, click ⋯ next to Quick Scan or System Scan and select **Edit**.

4. Customize the scan according to your needs and click **Next**.

5. Check the box next to **Choose when to schedule this task**, and then choose when the task should start.
   If you choose Daily, Monthly, or Weekly, drag the slider along the scale to set the desired period of time when the scheduled scan should start.

6. Click **Save**.

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

1. Click ⋯ next to the custom scan you created.

2. Click **Next** and then click **Next** again.

3. heck the box next to **Choose when to schedule this task**, and then choose when the task should start.

4. Click **Save**.

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

If there remain unresolved threats, you will be prompted to choose the actions to be taken on them. For more information, refer to Antivirus Scan Wizard (page 29).

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

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

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

To manage the proxy settings:

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

2. Select the **Advanced** tab.

3. Turn on **Proxy server**.

4. Click **Proxy change**.

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

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

   > **i** **Note**
   > Bitdefender can import proxy settings from the most popular browsers, including the latest versions of Microsoft Edge, Internet Explorer, Mozilla Firefox and Google Chrome.

   ❍ **Custom proxy settings** - proxy settings that you can configure yourself.
   The following settings must be specified:

      ❍ **Address** - type in the IP of the proxy server.

      ❍ **Port** - type in the port Bitdefender uses to connect to the proxy server.

      ❍ **Username** - type in a user name recognized by the proxy.

      ❍ **Password** - type in the valid password of the previously specified user.

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

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

Am I using a 32 bit or a 64 bit version of Windows?

To find out if you have a 32 bit or a 64 bit operating system:

❍ In **Windows 7**:

   1. Click **Start**.

   2. Locate **Computer** on the **Start** menu.

   3. Right-click **Computer** and select **Properties**.

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

❍ In **Windows 8.1**:

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

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

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

❍ In **Windows 10** and **Windows 11**:

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

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

How do I display hidden objects in Windows?

These steps are useful in those cases where you are dealing with a threat situation and you need to find and remove the infected files, which could be hidden.

Follow these steps to display hidden objects in Windows:

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

2. Select **Folder Options**.

3. Go to **View** tab.

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

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

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

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

In **Windows 10** and **Windows 11**:

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

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

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

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

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

How do I remove other security solutions?

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

When you use more than one security solution on the same device, the system becomes unstable. The Bitdefender Ultimate Small Business Security installer automatically detects other security programs and offers you the option to uninstall them.

If you did not remove the other security solutions during the initial installation:

❍ In **Windows 7**:

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

2. Wait a few moments until the installed software list is displayed.

3. Find the name of the program you want to remove and select **Uninstall**.

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

❍ In **Windows 8.1**:

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

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

3. Wait a few moments until the installed software list is displayed.

4. Find the name of the program you want to remove and select **Uninstall**.

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

❍ In **Windows 10** and **Windows 11**:

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

2. Click the **System** icon in the Settings area, then select **Apps**.

3. Find the name of the program you want to remove and select **Uninstall**.

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

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

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

How do I restart in Safe Mode?

Safe mode is a diagnostic operating mode, used mainly to troubleshoot problems affecting normal operation of Windows. Such problems range from conflicting drivers to threats preventing Windows from starting normally. In Safe Mode only a few apps work and Windows loads just the basic drivers and a minimum of operating system components. This is why most threats are inactive when using Windows in Safe Mode and they can be easily removed.

To start Windows in Safe Mode:

❍ In **Windows 7**:

1. Restart the device.

2. Press the **F8** key several times before Windows starts to access the boot menu.

3. Select **Safe Mode** in the boot menu or **Safe Mode with Networking** if you want to have internet access.

4. Press **Enter** and wait while Windows loads in Safe Mode.

5. This process ends with a confirmation message. Click **OK** to acknowledge.

6. To start Windows normally, simply reboot the system.

❍ In **Windows 8.1**, **Windows 10** and **Windows 11**:

1. Launch **System Configuration** in Windows by simultaneously pressing the **Windows + R** keys on your keyboard.

2. Write **msconfig** in the **Open** dialog box, then click **OK**.

3. Select the **Boot** tab.

4. In the **Boot options** area, select the **Safe boot** check box.

5. Click **Network**, and then **OK**.

6. Click **OK** in the **System Configuration** window which informs you that the system needs to be restarted to be able to make the changes you set.
   Your system is restarting in Safe Mode with Networking.

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

3.5. Troubleshooting

3.5.1. Solving common issues

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

❍ My system appears to be slow (page 116)

❍ Scan doesn't start (page 117)

❍ I can no longer use an app (page 119)

❍ What to do when Bitdefender blocks a website, a domain, an IP address, or an online app that is safe (page 120)

❍ How to update Bitdefender on a slow internet connection (page 125)

❍ Bitdefender services are not responding (page 125)

❍ Antispam filter does not work properly (page 126)

❍ Bitdefender removal failed (page 130)

❍ My system doesn't boot up after installing Bitdefender (page 132)

If you cannot find your problem here, or if the presented solutions do not solve it, you can contact the Bitdefender technical support representatives as presented in chapter Asking for Help (page 270).

My system appears to be slow

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

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

❍ **Bitdefender is not the only security program installed on the system**.
Though Bitdefender searches and removes the security programs found during the installation, it is recommended to remove any other security solution you may use before installing Bitdefender. For more information, refer to How do I remove other security solutions? (page 113).

❍ **The system requirements for running Bitdefender are not met.**
If your machine does not meet the system requirements, the device will become sluggish, especially when multiple apps are running at the same time. For more information, refer to System requirements (page 9).

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

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

❍ **Your system may be infected.**
Your system speed and its general behavior can also be affected by threats. Spyware, malware, Trojans and adware all take a toll on your device's performance. Make sure to scan your system periodically, at least once a week. It is recommended to use the Bitdefender System

Scan because it scans for all types of threats endangering the security of your system.

To start the System Scan:

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. In the **Scans** window, click **Run Scan** next to **System Scan**.

4. Follow the wizard steps.

Scan doesn't start

This type of issue can have two main causes:

❍ **A previous Bitdefender installation which was not completely removed or a faulty Bitdefender installation.**
In this case reinstall Bitdefender:

❍ In **Windows 7**:

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

2. Find **Bitdefender Ultimate Small Business Security** and select **Uninstall**.

3. Click **REINSTALL** in the window that appears.

4. Wait for the reinstall process to complete, and then reboot your system.

❍ In **Windows 8.1**:

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 Ultimate Small Business Security** and select **Uninstall**.

4. Click **REINSTALL** in the window that appears.

5. Wait for the reinstall process to complete, and then reboot your system.

❍ In **Windows 10** 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 Ultimate Small Business Security** and select **Uninstall**.

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

5. Click **REINSTALL** in the window that appears.

6. Wait for the reinstall process to complete, and then reboot your system.

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

❍ **Bitdefender is not the only security solution installed on your system.**
In this case:

1. Remove the other security solution. For more information, refer to How do I remove other security solutions? (page 113).

2. Reinstall Bitdefender:

   ❍ In **Windows 7**:

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

   b. Find **Bitdefender Ultimate Small Business Security** and select **Uninstall**.

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

   d. Wait for the reinstall process to complete, and then reboot your system.

❍ In **Windows 8.1**:

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

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

   c. Find **Bitdefender Ultimate Small Business Security** and select **Uninstall**.

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

   e. Wait for the reinstall process to complete, and then reboot your system.

❍ In **Windows 10** and **Windows 11**:

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

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

   c. Find **Bitdefender Ultimate Small Business Security** and select **Uninstall**.

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

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

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

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

If this information was not helpful, you can contact Bitdefender for support as described in section Asking for Help (page 270).

I can no longer use an app

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

After installing Bitdefender you may encounter one of these situations:

❍ You could receive a message from Bitdefender that the program is trying to make a modification to the system.

❍ You could receive an error message from the program you're trying to use.

This type of situation occurs when Advanced Threat Defense mistakenly detects some apps as malicious.

Advanced Threat Defense is a Bitdefender feature which constantly monitors the apps running on your system and reports those with potentially malicious behavior. Since this feature is based on a heuristic system, there may be cases when legitimate apps are reported by Advanced Threat Defense.

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

To add the program to the exceptions list:

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

2. In the **ADVANCED THREAT DEFENSE** pane, click **Open**.

3. In the **Settings** window, click **Manage Exceptions**.

4. Click **+Add an Exception**.

5. Enter the path of the executable you want to except from scanning in the corresponding field.
   Alternatively, you can navigate to the executable by clicking the browse button in the right side of the interface, select it and click on **OK**.

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

7. Click **Save**.

If this information was not helpful, you can contact Bitdefender for support as described in section Asking for Help (page 270).

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

Bitdefender offers a secure web browsing experience by filtering all web traffic and blocking any malicious content. However, it is possible that Bitdefender considers a website, a domain, an IP address, or online

app that are safe as unsafe, which will cause Bitdefender HTTP traffic scanning to block them incorrectly.

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

To add a website to **Exceptions**:

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

2. In the **ONLINE THREAT PREVENTION** pane, click **Settings**.

3. Click **Manage exceptions**.

4. Click **+Add an Exception**.

5. Type in the corresponding field the name of the website, the name of the domain, or the IP address you want to add to exceptions.

6. Click the switch next to **Online Threat Prevention**.

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

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

If this information was not helpful, you can contact Bitdefender for support as described in section Asking for Help (page 270).

I cannot connect to the internet

You may notice that a program or a web browser can no longer connect to the internet or access network services after installing Bitdefender.

In this case, the best solution is to configure Bitdefender to automatically allow connections to and from the respective software app:

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

2. In the **FIREWALL** pane, click **Settings**.

3. In the **Rules** window, click **Add rule**.

4. A new window appears where you can add the details. Make sure to select all the network types available and in the **Permission** section select **Allow**.

Close Bitdefender, open the software app and try again to connect to the internet.

If this information was not helpful, you can contact Bitdefender for support as described in section Asking for Help (page 270).

I cannot access a device on my network

Depending on the network you are connected to, the Bitdefender firewall may block the connection between your system and another device (such as another PC or a printer). As a result, you may no longer share or print files.

In this case, the best solution is to configure Bitdefender to automatically allow connections to and from the respective device, as follows:

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

2. In the **FIREWALL** pane, click **Settings**.

3. In the **Rules** window, click **Add rule**.

4. Turn on the **Apply this rule to all applications** option.

5. Click the **Advanced Settings** button.

6. In the **Custom Remote Address** box, type the IP address of the PC or printer you want to have unrestricted access to.

If you still cannot connect to the device, the issue may not be caused by Bitdefender.

Check for other potential causes, such as the following:

❍ The firewall on the other device may block file and printer sharing with your PC.

   ❍ If the Windows Firewall is used, it can be configured to allow file and printer sharing as follows:

      ❍ In **Windows 7**:

         1. Click **Start**, go to **Control Panel** and select **System and Security**.

         2. Go to **Windows Firewall**, and then click **Allow a program through Windows Firewall**.

         3. Select the **File and Printer Sharing** check box.

❍ In **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 **System and Security**, go to **Windows Firewall** and select **Allow an app through Windows Firewall**.

3. Select the **File and Printer Sharing** check box, and then click **OK**.

❍ In **Windows 10** and **Windows 11**:

1. Type "Allow an app through Windows Firewall" in the search box from the taskbar and click its icon.

2. Click **Change settings**.

3. In the **Allowed apps and features** list select the **File and Printer Sharing** check box, and then click **OK**.

❍ If another firewall program is used, refer to its documentation or help file.

❍ General conditions that may prevent using or connecting to the shared printer:

❍ You may need to log on to a Windows administrator account to access the shared printer.

❍ Permissions are set for the shared printer to allow access to specific device and users only. If you are sharing your printer, check the permissions set for the printer to see if the user on the other device is allowed access to the printer. If you are trying to connect to a shared printer, check with the user on the other device if you have permission to connect to the printer.

❍ The printer connected to your device or to the other one is not shared.

❍ The shared printer is not added on the device.

> **i** **Note**
> To learn how to manage printer sharing (share a printer, set or remove permissions for a printer, connect to a network printer or to a shared printer), go to the Windows Help and Support Center (in the Start menu, click **Help and Support**).

❍ Access to a network printer may be restricted to specific devices or users only. You should check with the network administrator if you have permission to connect to that printer.

If this information was not helpful, you can contact Bitdefender for support as described in section Asking for Help (page 270).

My internet is slow

This situation may appear after you install Bitdefender. The issue could be caused by errors in the Bitdefender firewall configuration.

To troubleshoot this situation:

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

2. In the **FIREWALL** pane, turn off the switch to disable the feature.

3. Check if your internet connection improved with the Bitdefender firewall disabled.

   ❍ If you still have a slow internet connection, the issue may not be caused by Bitdefender. You should contact your Internet Service Provider to verify if the connection is operational on their side.

   If you receive confirmation from your Internet Service Provider that the connection is operational on their side and the issue still persists, contact Bitdefender as described in section Asking for Help (page 270).

   ❍ If the internet connection improved after disabling the Bitdefender firewall:

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

   b. In the **FIREWALL** pane, click **Settings**.

   c. Go to the **Network Adapters** tab and set your internet connection on **Home/Office**.

   d. In the **Settings** tab, turn off **Port scan protection**.

In the **Stealth Mode** area, click **Edit stealth settings**. Turn on Stealth Mode for the network adapter you are connected to.

e. Close Bitdefender, reboot the system and check the internet connection speed.

If this information was not helpful, you can contact Bitdefender for support as described in section .

How to update Bitdefender on a slow internet connection

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

To keep your system up to date with the latest Bitdefender threat information database:

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

2. Select the **Update** tab.

3. Turn off the **Silent update** switch.

4. Next time when an update will be available, you will be prompted to select which update you would like to download. Select only **Signatures update**.

5. Bitdefender will download and install only the threat information database.

Bitdefender services are not responding

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

❍ The Bitdefender icon in the system tray is grayed out and you are informed that the Bitdefender services are not responding.

❍ The Bitdefender window indicates that the Bitdefender services are not responding.

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

❍ temporary communication errors between the Bitdefender services.

❍ some of the Bitdefender services are stopped.

❍ other security solutions running on your device at the same time with Bitdefender.

To troubleshoot this error, try these solutions:

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

2. Restart the device and wait a few moments until Bitdefender is loaded. Open Bitdefender to see if the error persists. Restarting the device usually solves the problem.

3. Check if you have any other security solution installed as they may disrupt the normal operation of Bitdefender. If this is the case, we recommend you to remove all of the other security solutions and then reinstall Bitdefender.

   For more information, refer to How do I remove other security solutions? (page 113).

If the error persists, please contact our support representatives for help as described in section Asking for Help (page 270).

Antispam filter does not work properly

This article helps you troubleshoot the following problems concerning the Bitdefender Antispam filtering operation:

❍ A number of legitimate email messages are marked as [spam].

❍ Many spam messages are not marked accordingly by the antispam filter.

❍ The antispam filter does not detect any spam message.

Legitimate messages are marked as [spam]

Legitimate messages are marked as [spam] simply because they look like spam to the Bitdefender antispam filter. You can normally solve this problem by adequately configuring the Antispam filter.

Bitdefender automatically adds the receivers of your email messages to a Friends List. The email messages received from the contacts in the Friends list are considered to be legitimate. They are not verified by the antispam filter and, thus, they are never marked as [spam].

The automatic configuration of the Friends list does not prevent the detection errors that may occur in these situations:

❍ You receive a lot of solicited commercial mail as a result of subscribing on various websites. In this case, the solution is to add the email addresses from which you receive such email messages to the Friends list.

❍ A significant part of your legitimate mail is from people to whom you never e-mailed before, such as customers, potential business partners and others. Other solutions are required in this case.

If you are using one of the mail clients Bitdefender integrates into, indicate detection errors.

> **ⓘ** Note
> Bitdefender integrates into the most commonly used mail clients through an easy-to-use antispam toolbar. For a complete list of supported mail clients, refer to Supported email clients and protocols (page 45).

Add contacts to Friends List

If you are using a supported mail client, you can easily add the senders of legitimate messages to the Friends list. Follow these steps:

1. In your mail client, select an email message from the sender that you want to add to the Friends list.

2. Click the 📩 **Add Friend** button on the Bitdefender antispam toolbar.

3. You may be asked to acknowledge the addresses added to the Friends list. Select **Don't show this message again** and click **OK**.

You will always receive email messages from this address no matter what they contain.

If you are using a different mail client, you can add contacts to the Friends list from the Bitdefender interface. Follow these steps:

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

2. In the **ANTISPAM** pane, click **Manage Friends**.
   A configuration window appears.

3. Type the email address you always want to receive email messages from and then click **ADD**. You can add as many email addresses as you want.

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

Indicate detection errors

If you are using a supported mail client, you can easily correct the antispam filter (by indicating which email messages should not have been marked as *[spam]*). Doing so helps improve the efficiency of the antispam filter. Follow these steps:

1. Open your mail client.

2. Go to the junk mail folder where spam messages are moved.

3. Select the legitimate message incorrectly marked as *[spam]* by Bitdefender.

4. Click the ⚐ **Add Friend** button on the Bitdefender antispam toolbar to add the sender to the Friends list. You may need to click **OK** to acknowledge. You will always receive email messages from this address no matter what they contain.

5. Click the ⚐ **Not Spam** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window). The email message will be moved to the Inbox folder.

Many spam messages are not detected

If you are receiving many spam messages that are not marked as [spam], you must configure the Bitdefender antispam filter so as to improve its efficiency.

Try the following solutions:

1. If you are using one of the mail clients Bitdefender integrates into, indicate undetected spam messages.

> **ⓘ Note**
> Bitdefender integrates into the most commonly used mail clients through an easy-to-use antispam toolbar. For a complete list of supported mail clients, refer to Supported email clients and protocols (page 45).

2. Add spammers to the Spammers list. The email messages received from addresses in the Spammers list are automatically marked as [spam].

Indicate undetected spam messages

If you are using a supported mail client, you can easily indicate which email messages should have been detected as spam. Doing so helps improve the efficiency of the antispam filter. Follow these steps:

1. Open your mail client.

2. Go to the Inbox folder.

3. Select the undetected spam messages.

4. Click the ⊠ **Is Spam** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window). They are immediately marked as [spam] and moved to the junk mail folder.

Add spammers to Spammers List

If you are using a supported mail client, you can easily add the senders of the spam messages to the Spammers list. Follow these steps:

1. Open your mail client.

2. Go to the junk mail folder where spam messages are moved.

3. Select the messages marked as *[spam]* by Bitdefender.

4. Click the ⊠ **Add Spammer** button on the Bitdefender antispam toolbar.

5. You may be asked to acknowledge the addresses added to the Spammers list. Select **Don't show this message again** and click **OK**.

If you are using a different mail client, you can manually add spammers to the Spammers list from the Bitdefender interface. It is convenient to do this only when you have received several spam messages from the same email address. Follow these steps:

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

2. In the **ANTISPAM** pane, click **Settings**.

3. Go to the **Manage Spammers** window.

4. Type the spammer's email address and then click the **Add**. You can add as many email addresses as you want.

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

Antispam filter does not detect any spam message

If no spam message is marked as [spam], there may be a problem with the Bitdefender Antispam filter. Before troubleshooting this problem, make sure it is not caused by one of the following conditions:

❍ Antispam protection might be turned off. To verify the antispam protection status, click **Protection** on the navigation menu on the Bitdefender interface. Look in the **Antispam** pane to check if the feature is enabled.
If Antispam is turned off, this is what is causing your problem. Click the corresponding switch to turn on your antispam protection.

❍ The Bitdefender Antispam protection is available only for email clients configured to receive email messages via the POP3 protocol. This means the following:

  ❍ Email messages received via web-based email services (such as Yahoo, Gmail, Hotmail or other) are not filtered for spam by Bitdefender.

  ❍ If your email client is configured to receive email messages using other protocol than POP3 (for example, IMAP4), the Bitdefender Antispam filter does not check them for spam.

  ⓘ Note
  POP3 is one of the most widely used protocols for downloading email messages from a mail server. If you do not know the protocol that your email client uses to download email messages, ask the person who configured your email client.

❍ Bitdefender Ultimate Small Business Security doesn't scan Lotus Notes POP3 traffic.

A possible solution is to repair or reinstall the product. However, you may want to contact Bitdefender for support instead, as described in section Asking for Help (page 270).

Bitdefender removal failed

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

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

To completely remove Bitdefender from your system:

❍ In **Windows 7**:

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

2. Find **Bitdefender Ultimate Small Business Security** and select **Uninstall**.

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

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

❍ In **Windows 8.1**:

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 Ultimate Small Business Security** and select **Uninstall**.

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

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

❍ In **Windows 10** 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 Ultimate Small Business Security** and select **Uninstall**.

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

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

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

My system doesn't boot up after installing Bitdefender

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

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

This is how you may address each situation:

❍ **You had Bitdefender before and you did not remove it properly.**
To solve this:

1. Reboot your system and enter in Safe Mode. To find out how to do this, refer to How do I restart in Safe Mode? (page 114).

2. Remove Bitdefender from your system:

❍ In **Windows 7**:

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

b. Find **Bitdefender Ultimate Small Business Security** and select **Uninstall**.

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

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

e. Reboot your system in normal mode.

❍ In **Windows 8.1**:

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

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

c. Find **Bitdefender Ultimate Small Business Security** and select **Uninstall**.

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

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

      f. Reboot your system in normal mode.

❍ In **Windows 10** and **Windows 11**:

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

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

      c. Find **Bitdefender Ultimate Small Business Security** and select **Uninstall**.

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

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

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

      g. Reboot your system in normal mode.

3. Reinstall your Bitdefender product.

❍ **You had a different security solution before and you did not remove it properly.**
To solve this:

1. Reboot your system and enter in Safe Mode. To find out how to do this, refer to .

2. Remove the other security solution from your system:

❍ In **Windows 7**:

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

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

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

❍ In **Windows 8.1**:

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

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

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

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

❍ In **Windows 10** and **Windows 11**:

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

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

    c. Find the name of the program you want to remove and select **Uninstall**.

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

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

3. Reboot your system in normal mode and reinstall Bitdefender.

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

To solve this:

1. Reboot your system and enter in Safe Mode. To find out how to do this, refer to How do I restart in Safe Mode? (page 114).

2. Use the System Restore option from Windows to restore the device to an earlier date before installing the Bitdefender product.

3. Reboot the system in normal mode and contact our support representatives for help as described in section Asking for Help (page 270).

3.5.2. Removing threats from your system

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

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

❍ Rescue Environment (page 135)

❍ What to do when Bitdefender finds threats on your device? (page 136)

❍ How do I clean a threat in an archive? (page 137)

❍ How do I clean a threat in an email archive? (page 138)

❍ What to do if I suspect a file as being dangerous? (page 139)

❍ What are the password-protected files in the scan log? (page 140)

❍ What are the skipped items in the scan log? (page 140)

❍ What are the over-compressed files in the scan log? (page 140)

❍ Why did Bitdefender automatically delete an infected file? (page 140)

If you cannot find your problem here, or if the presented solutions do not solve it, you can contact the Bitdefender technical support representatives as presented in chapter Asking for Help (page 270).

Rescue Environment

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

Bitdefender Rescue Environment is integrated with Windows RE.

Starting your system in Rescue Environment

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

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

2. In the **ANTIVIRUS** pane, click **Open**.

3. Click **Open** next to **Rescue Environment**.

4. Click **REBOOT** in the window that appears.
   Bitdefender Rescue Environment loads in a few moments.

Scanning your system in Rescue Environment

To scan your system Rescue Environment:

1. Enter Rescue Environment, as described in Starting your system in Rescue Environment (page 135).

2. The Bitdefender scanning process starts automatically as soon as the system is loaded in Rescue Environment.

3. Wait for the scan to complete. If any threat is detected, follow the instructions to remove it.

4. To exit Rescue Environment, click the Close button in the window with the scan results.

What to do when Bitdefender finds threats on your device?

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

❍ You scanned your device and Bitdefender found infected items on it.

❍ A threat alert informs you that Bitdefender blocked one or multiple threats on your device.

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

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

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

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

The first method can be used in normal mode:

1. Turn off the Bitdefender real-time antivirus protection:

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

b. In the **ANTIVIRUS** pane, click **Open**.

c. In the **Advanced** window, turn off **Bitdefender Shield**.

2. Display hidden objects in Windows. To find out how to do this, refer to How do I display hidden objects in Windows? (page 112).

3. Browse to the location of the infected file (check the scan log) and delete it.

4. Turn on the Bitdefender real-time antivirus protection.

In case the first method failed to remove the infection:

1. Reboot your system and enter in Safe Mode. To find out how to do this, refer to How do I restart in Safe Mode? (page 114).

2. Display hidden objects in Windows. To find out how to do this, refer to How do I display hidden objects in Windows? (page 112).

3. Browse to the location of the infected file (check the scan log) and delete it.

4. Reboot your system and enter in normal mode.

If this information was not helpful, you can contact Bitdefender for support as described in section Asking for Help (page 270).

How do I clean a threat in an archive?

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

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

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

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

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

1. Identify the archive that includes the threat by performing a System Scan of the system.

2. Turn off the Bitdefender real-time antivirus protection:

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

   b. In the **ANTIVIRUS** pane, click **Open**.

   c. In the **Advanced** window, turn off **Bitdefender Shield**.

3. Go to the location of the archive and decompress it using an archiving app, like WinZip.

4. Identify the infected file and delete it.

5. Delete the original archive to make sure the infection is totally removed.

6. Recompress the files in a new archive using an archiving app, like WinZip.

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

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

If this information was not helpful, you can contact Bitdefender for support as described in section Asking for Help (page 270).

How do I clean a threat in an email archive?

Bitdefender can also identify threats in email databases and email archives stored on disk.

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

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

1. Scan the email database with Bitdefender.

2. Turn off the Bitdefender real-time antivirus protection:

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

b. In the **ANTIVIRUS** pane, click **Open**.

c. In the **Advanced** window, turn off **Bitdefender Shield**.

3. Open the scan report and use the identification information (Subject, From, To) of the infected messages to locate them in the email client.

4. Delete the infected messages. Most email clients also move the deleted message to a recovery folder, from which it can be recovered. You should make sure the message is deleted also from this recovery folder.

5. Compact the folder storing the infected message.

❍ In Microsoft Outlook 2007: On the File menu, click Data File Management. Select the personal folders (.pst) files you intend to compact, and click Settings. Click Compact Now.

❍ In Microsoft Outlook 2010 / 2013/ 2016: On the File menu, click Info, and then Account settings (Add and remove accounts or change existing connection settings). Then click Data File, select the personal folders (.pst) files you intend to compact, and click Settings. Click Compact Now.

6. Turn on the Bitdefender real-time antivirus protection.

If this information was not helpful, you can contact Bitdefender for support as described in section Asking for Help (page 270).

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

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

To make sure your system is protected:

1. Run a **System Scan** with Bitdefender. To find out how to do this, refer to How do I scan my system (page 97).

2. If the scan result appears to be clean, but you still have doubts and want to make sure about the file, contact our support representatives so that we may help you.
To find out how to do this, refer to Asking for Help (page 270).

What are the password-protected files in the scan log?

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

Most commonly, the password-protected items are:

❍ Files that belong to another security solution.

❍ Files that belong to the operating system.

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

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

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

What are the skipped items in the scan log?

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

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

What are the over-compressed files in the scan log?

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

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

Why did Bitdefender automatically delete an infected file?

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

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

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

4. ANTIVIRUS FOR MAC

4.1. 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.

4.2. Installation and Removal

This chapter includes the following topics:

4.2.1. 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.

> **i** 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.

4.2.2. 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.

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
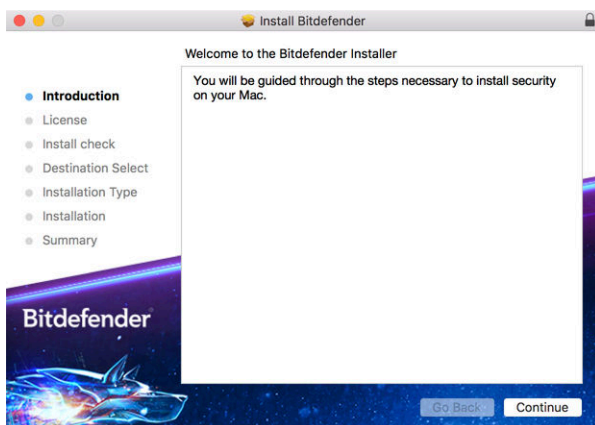
Click **Continue**.

Step 2 - Read the Subscription Agreement
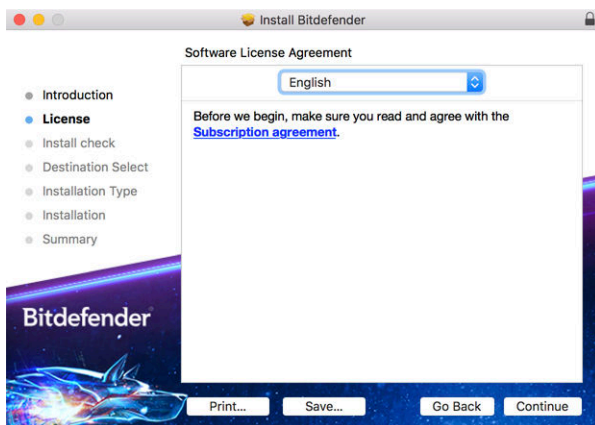
Before continuing with the installation, you have to agree with the Subscription Agreement. Please take some time to read the Subscription Agreement as it contains the terms and conditions under which you may use Bitdefender Antivirus for Mac.

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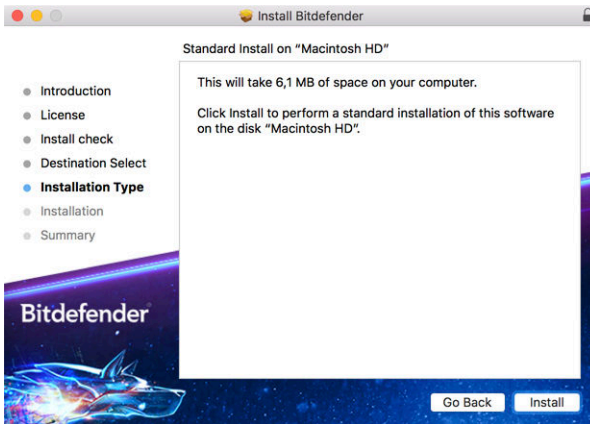
Bitdefender Antivirus for Mac will be installed in Macintosh HD/Library/ Bitdefender. The installation path cannot be changed.

Click **Install** to start the installation.

Step 4 - Installing Bitdefender Antivirus for Mac
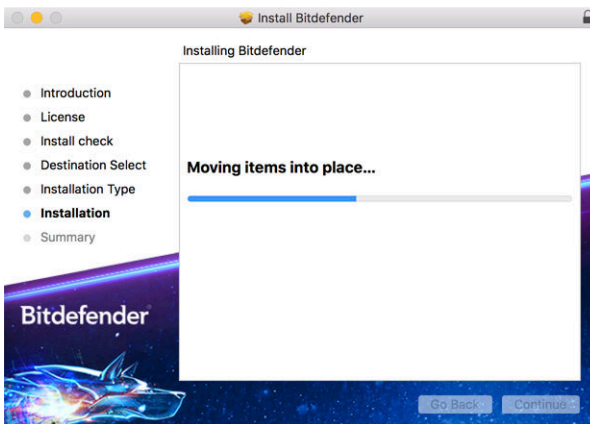
Wait until the installation is completed, and then click **Continue**.

Step 5 - Finish
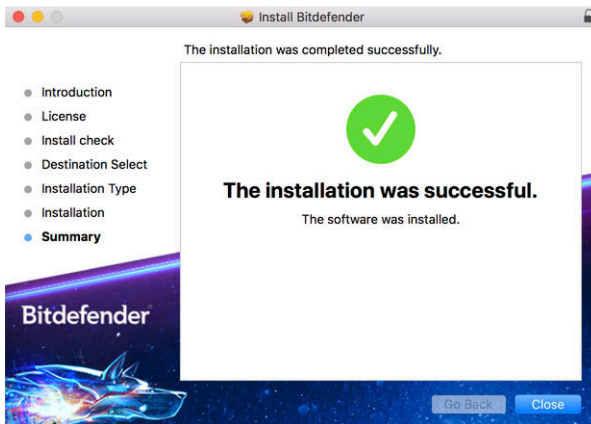
Click **Close** to close the installer window.

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.

4.2.3. 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.

> **i** **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 270).

4.3. Getting Started

This chapter includes the following topics:

4.3.1. 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.

4.3.2. 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.
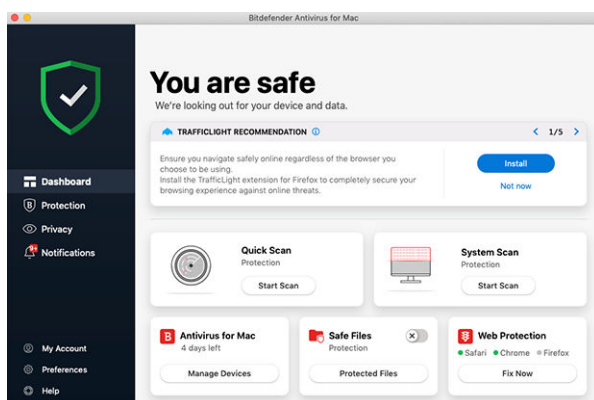
To go through the Bitdefender interface, an introduction wizard containing details on how to interact with the product and how to configure it is displayed on the upper left side. Select the right angle bracket to continue being guided, or **Skip tour** to close the wizard.

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 164).

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.

4.3.3. 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.
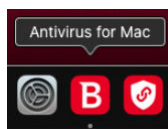
4.3.4. Navigation Menu

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.

4.3.5. 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.
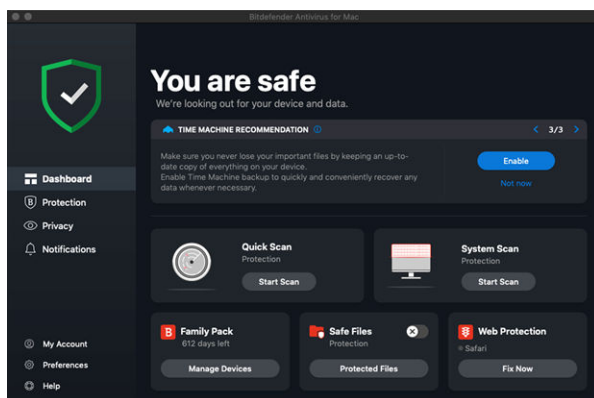
4.4. Protecting against Malicious Software

This chapter includes the following topics:

4.4.1. 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 164).

❍ 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 165).

❍ 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 167).

4.4.2. 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.

> **i** 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.

4.4.3. Scan Wizard

Whenever you initiate a scan, the Bitdefender Antivirus for Mac scan wizard will appear.
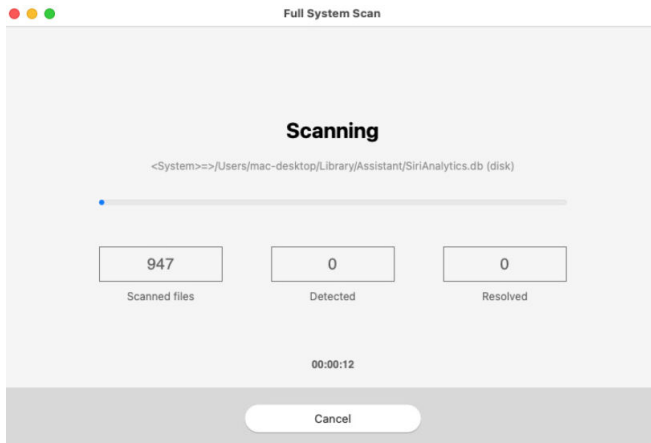
Real-time information about detected and resolved threats is displayed during each Scan.

Wait for Bitdefender Antivirus for Mac to finish scanning.

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

4.4.4. 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.
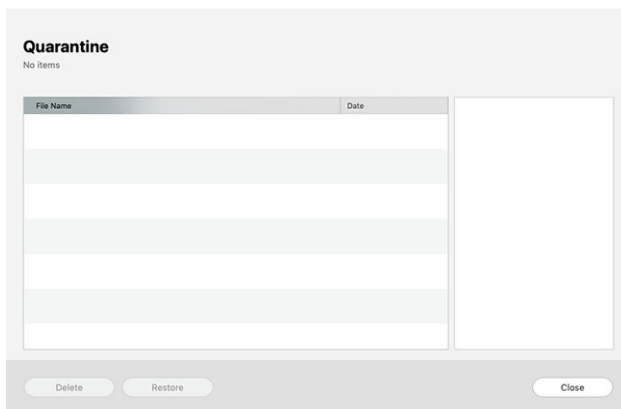
The Quarantine section displays all the files currently isolated in the Quarantine folder.

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.

4.4.5. 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.

4.4.6. Scam Copilot for macOS

Scam Copilot is Bitdefender's AI-powered scam detector.

In using it, you can send any tricky texts, emails, social media messages, links or even QR codes you've received and are suspicious of, in order to get an instant analysis on their safety and legitimacy.

To set up Scam Copilot:

1. Open Bitdefender Antivirus for Mac.

2. In the main dashboard:

   ❍ Click on the **Scam Copilot** panel directly, or

   ❍ Click on **Protection** in the left side menu, then open the **Scam Copilot** tab at the top.

3. Click on the **Get started** button.

4. Set up Scam Copilot.
   You will see which Scam Copilot components are already enabled and which are not, and you will be guided to configure those that need extra steps. Follow the on-screen instructions to grant the required permissions:

   ❍ **Online Scam Protection:**

      a. Click the **Enable extension** button.

      b. Install the TrafficLight (page 158) extension in your browser, if you haven't already.

   ❍ **New Scam Wave Alerts:**

      a. Click the **Allow notification permission** button to receive alerts about emerging scam campaigns in your region.

   ❍ **Email Protection**

    a. If Email Protection is disabled, click the **Add email account** button.

    b. Choose your email provider. (Google or Outlook)

    c. Sign in with your Google or Outlook email account.

    d. Allow Bitdefender to scan your mailbox.

5. Once all Scam Copilot components are enabled, you can close the setup window.

Scam Copilot for your macOS is now successfully configured!

4.4.7. 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
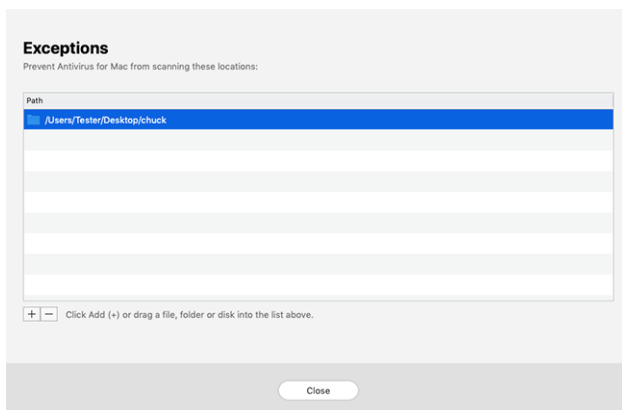
The exceptions list contains the paths that have been excepted from scanning.

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.

4.4.8. 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.

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.

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.

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.

4.4.9. 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.

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.

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.

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.

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 ⊕ .

4.4.10. 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**
> (i) 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.

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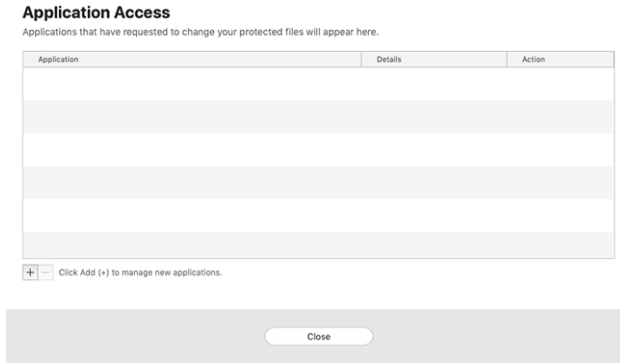
1. Click **Protection** on the navigation menu on the Bitdefender interface.

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.

Application Access
Applications that have requested to change your protected files will appear here.

Application	Details	Action

+ — Click Add (+) to manage new applications.

Close

4.4.11. 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.

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.

4.4.12. 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.
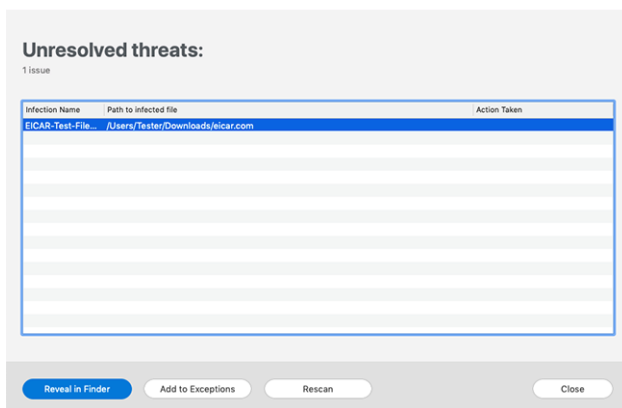
The list of unresolved threats is updated after each system scan no matter whether the scan is automatically made in the background or initiated by you.

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.

4.4.13. 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.

4.4.14. 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.

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.

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.

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.

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**.

4.5. Configuring Preferences

This chapter includes the following topics:

4.5.1. 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**.

4.5.2. 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.

4.5.3. 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.

4.5.4. 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.

4.6. 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 270).

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.

5. MOBILE SECURITY FOR ANDROID

5.1. What is Bitdefender Mobile Security

Online activities such as paying bills, making holiday reservations, or buying goods and services are convenient and hassle-free. But as many activities evolved on the internet, these come with high risks and, if security details are ignored, personal data may be hacked. And what is more important than protecting data stored in online accounts and on the personal smartphone?

Bitdefender Mobile Security allows you to:

❍ Gain the best protection for your Android smartphone and tablet with minimal impact on battery life

❍ Protect yourself from falling victim to link-based mobile scams

❍ Have access to our secure VPN for a fast, anonymous and safe experience while surfing the web

❍ Remotely locate, lock and wipe your Android device in case of loss or theft

❍ Verify whether your email account has been involved in data breakages or data leaks

5.2. Getting Started

5.2.1. Device Requirements

Bitdefender Mobile Security works on any device running Android 5.0 or any later versions of the operating system. An active internet connection is required for in-the-cloud threat scanning.

5.2.2. Installing Bitdefender Mobile Security

❍ **From Bitdefender Central**

  ❍ On Android

    1. Go to: https://central.bitdefender.com.

    2. Sign in to your Bitdefender account.

3. Select the **My Devices** panel.

4. Tap **INSTALL PROTECTION**, and then tap **Protect this device**.

5. Select the owner of the device. If the device belongs to someone else, tap the corresponding button.

6. You are redirected to the **Google Play** app. In the Google Play screen, tap the installation option.

❍ On Windows, macOS, and iOS

1. Go to: https://central.bitdefender.com.

2. Sign in to your Bitdefender account.

3. Select the **My Devices** panel.

4. Press **INSTALL PROTECTION**, and then press **Protect other devices**.

5. Select the owner of the device. If the device belongs to someone else, press the corresponding button.

6. Press **SEND DOWNLOAD LINK**.

7. Type an email address in the corresponding field, and press **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.

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

❍ **From Google Play**
Search for Bitdefender Mobile Security to locate and install the app.
Alternatively, scan the QR Code:

Before going through the validation steps, 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 Mobile Security.
Tap **CONTINUE** to proceed to the next window.

5.2.3. Sign in to your Bitdefender account

To use Bitdefender Mobile Security, you must link your device to a Bitdefender, Facebook, Google, Microsoft, or Apple account by signing in to the account from the app. The first time you open the app, you will be prompted to sign in to an account.

If you installed Bitdefender Mobile Security from your Bitdefender account, the app will attempt to automatically sign in to that account.

To link your device to a Bitdefender account:

1. Type your Bitdefender account email address and password in the corresponding fields. If you do not have a Bitdefender account and want to create one, select the corresponding link.

2. Tap **SIGN IN**.

To sign in using a Facebook, Google, or Microsoft account, tap the service you want to use from the OR SIGN WITH area. You are redirected to the login page of the selected service. Follow the instructions to link your account to Bitdefender Mobile Security.

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

5.2.4. Configure Protection

Once you successfully sign in to the app, the Configure protection window appears. To secure your device, we recommend you to go through these steps:

❍ **Subscription status**. To be protected by Bitdefender Mobile Security, you must activate your product with a subscription, which specifies how long you may use the product. As soon as it expires, the app stops performing its functions and protecting your device.
If you have an activation code, tap I **HAVE A CODE**, and then tap **ACTIVATE**.
If you have signed in with a new Bitdefender account and have no activation code, you can use the product for 14 days, free of charge.

❍ **Web Protection**. If your device requires Accessibility to activate Web Protection, tap **ACTIVATE**. You are redirected to the Accessibility

menu. Tap Bitdefender Mobile Security, and then turn on the corresponding switch.

❍ **Malware Scanner**. Run a one-time scan to make sure that your device is free from threats. To initiate the scan process, tap **SCAN NOW**.

As soon as the scanning process begins, the dashboard appears. Here you can see the security status of your device.

5.2.5. Dashboard

Tap the Bitdefender Mobile Security icon in your device's app drawer to open the app interface.

The Dashboard offers information about the security status of your device and through Autopilot helps you to improve your device security by giving you features recommendations.

The status card at the top of the window informs you about the device's security status using explicit messages and suggestive colors. If Bitdefender Mobile Security has no warnings, the status card is green. When a security issue has been detected, the status card changes its color into red.

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, Bitdefender Autopilot will come up with contextual recommendations based on your device usage and needs. This will help you discover and benefit from the advantages brought by the features included into the Bitdefender Mobile Security app.

Whenever there is a process in progress or a feature requires your input, a card with more information and possible actions is displayed in the Dashboard.

You can access the Bitdefender Mobile Security features and easily navigate from the bottom navigation bar:

Malware Scanner

Allows you to initiate an on-demand scan and enable Scan Storage. For more information, refer to Malware Scanner (page 179).

Web Protection

Ensures a safe browsing experience by alerting you about potential malicious webpages. For more information, refer to Web Protection (page 181).

VPN

Encrypts internet communication, helping you maintain your privacy no matter what network you are connected to. For more information, refer to VPN (page 183).

Scam Alert

Keeps you safe by alerting you of malicious links arriving via SMS, messaging applications and any type of notification. For more information, refer to Scam Alert (page 186).

Anti-Theft

Allows you to turn the Anti-Theft features on or off and to configure Anti-Theft settings. For more information, refer to Anti-Theft Features (page 188).

Account Privacy

Checks if any data breach has occurred in your online accounts. For more information, refer to Account Privacy (page 191).

App Lock

Allows you to protect your installed apps by setting a PIN access code. For more information, refer to App Lock (page 193).

Reports

Keeps a log of all important actions, status changes and other critical messages related to your device 's activity. For more information, refer to Reports (page 197).

WearON

Communicates with your smartwatch to help you find your phone in case you misplace or forget where you left it. For more information, refer to WearON (page 198).
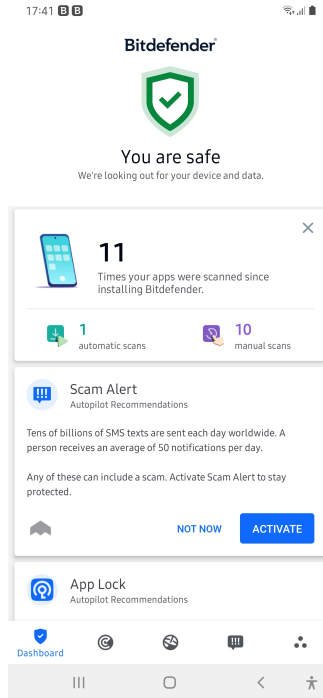
5.3. Malware Scanner

Bitdefender protects your device and data against malicious apps using on-install scanning and on-demand scanning.

The Malware Scanner interface provides a listo of all the types of threats Bitdefender looks for, along with their definitions. Simply tap on any threat to view its definition.

> **Note**
> Make sure your mobile device is connected to the internet. If your device is not connected to the internet, the scan process will not start.

❍ **On-install scanning**
Whenever you install an app, Bitdefender Mobile Security automatically scans it using in-the-cloud technology. The same scanning process starts each time the installed apps are updated.

If the app is found to be malicious, an alert will appear prompting you to uninstall it. Tap **Uninstall** to go to that app's uninstall screen.

❍ **On-demand scanning**
Whenever you want to make sure that the apps installed on your device are safe to use, you can initiate an on-demand scan.
To start an On-demand scan:

1. Tap **Malware Scanner** on the bottom navigation bar.

2. Tap **START SCAN**.

> (i) **Note**
> Additional permissions are required on Android 6 for the Malware Scanner feature. After tapping **START SCAN**, select **Allow** for the following:
>
> ❍ Allow **Antivirus** to make and manage phone calls?
>
> ❍ Allow **Antivirus** to access photos, media, and files on your device?

The scan progress is displayed and you can stop the process at any time.

By default, Bitdefender Mobile Security will scan your device's internal storage, including any mounted SD card. This way, any dangerous apps that might be on the card can be detected before they can cause harm.

To disable the Scan Storage setting:

1. Tap **More** on the bottom navigation bar.

2. Tap **Settings**.

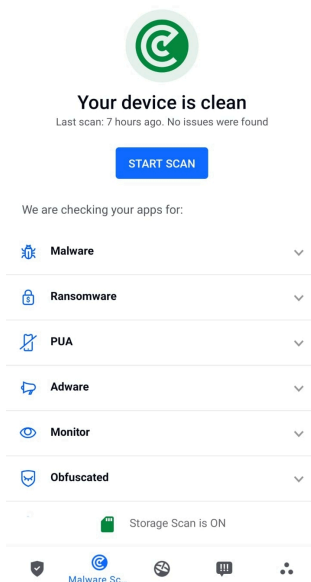3. Disable the **Scan Storage** switch in the Malware Scanner area.

If any malicious apps are detected, information about them will be displayed and you can remove them by tapping **UNINSTALL**.

The Malware Scanner card displays the state of your device. When your device is safe, the card is green. When the device requires a scan, or there is any action that requires your input, the card will turn red.

If your Android's version is 7.1 or newer, you can access a shortcut to Malware Scanner so that you can run scans faster, without opening the Bitdefender Mobile Security interface. To do this, press and hold the

Bitdefender icon on your Home screen or Apps drawer, and then select the ⓒ icon.

Your device is clean
Last scan: 7 hours ago. No issues were found

START SCAN

We are checking your apps for:

Malware

Ransomware

PUA

Adware

Monitor

Obfuscated

Storage Scan is ON

Malware Sc...

5.3.1. App Anomaly Detection

Bitdefender App Anomaly Detection is a novel technology integrated into the Bitdefender Malware Scanner to provide an additional layer of protection by continuously monitoring and detecting any malicious behaviors and alerting the user if suspicious activities are identified.

Bitdefender App Anomaly Detection protects users even when they have unknowingly installed a dangerous app that runs dormant for a period of time or a seemingly trusted app that breaks its functionality and turns rogue.

5.4. Web Protection

Web Protection checks using Bitdefender cloud services webpages you access with the default Android browser, Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Yandex Browser, Huawei Browser and Dolphin.

> **Note**
> Additional permissions are required on Android 6 for the Web Protection feature.
>
> Allow permission to register as Accessibility service and tap **TURN ON** when requested. Tap **Antivirus** and enable the switch, then confirm that you agree with the access to your device's permission.
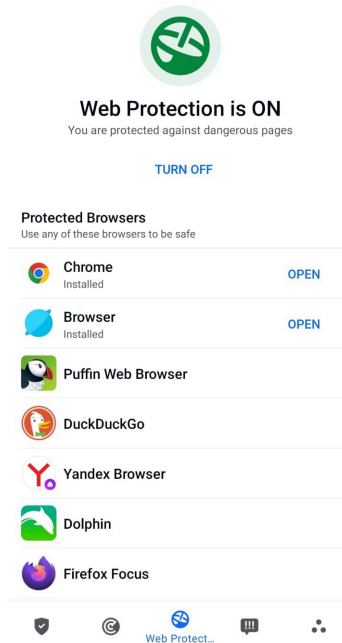
Each time you access a banking site, Bitdefender Web Protection is set to notify you to use Bitdefender VPN. The notification appears in the status bar. We recommend you to use Bitdefender VPN while you are signed in into your bank account so that your data can stay safe from potential security breaches.

To disable the Web Protection notification:

1. Tap ⁘ **More** on the bottom navigation bar.

2. Tap ⚙ **Settings**.

3. Turn off the corresponding switch in the Web Protection area.

5.5. 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 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 VPN, you are able to access content that is normally restricted in specific areas.

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

There are two ways to turn on or off Bitdefender VPN:

❍ Tap **CONNECT** in the VPN card from the Dashboard.
The status of Bitdefender VPN is displayed.

❍ Tap **VPN** on the bottom navigation bar, and then tap **CONNECT**.
Tap **CONNECT** each time you want to stay protected while connected to unsecured wireless networks.
Tap **DISCONNECT** whenever you want to disable the connection.

> **Note**
> The first time you turn on VPN, you are asked to allow Bitdefender to set up a VPN connection that will monitor network traffic. Tap **OK** to continue.

If your Android's version is 7.1 or newer, you can access a shortcut to Bitdefender VPN, without opening the Bitdefender Mobile Security interface.

To do this, press and hold the Bitdefender icon on your Home screen or Apps drawer, and then select the 🛡 icon.

To save battery power, we recommend you to turn off the VPN feature when you do not need it.

If you have a premium subscription and would like to connect to a server at your will, tap Server Location in the VPN feature, and then select the location you want. For details about VPN subscriptions, refer to
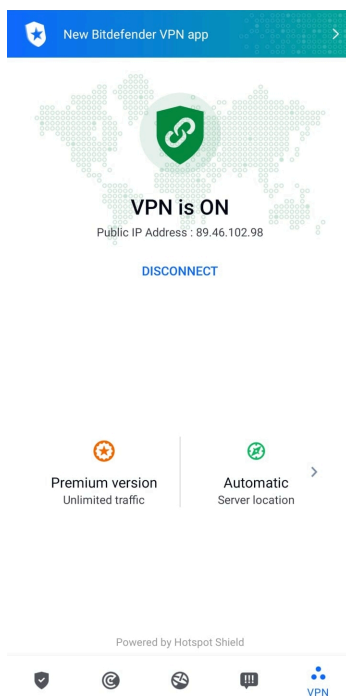
5.5.1. VPN Settings

For an advanced configuration of your VPN:

1. Tap ⠂⠂ **More** on the bottom navigation bar.

2. Tap ✿ **Settings**.

In the VPN area, you can configure the following options:

❍ Quick VPN access - a notification will appear in the status bar of your device to allow you to quickly turn on VPN.

❍ Open Wi-Fi warning - each time you connect to an open Wi-Fi network, you are notified in the status bar of your device to use VPN.

5.5.2. Subscriptions

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

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

You can upgrade to the Bitdefender Premium VPN version anytime by tapping on **Activate Premium** in the VPN window.

The Bitdefender Premium VPN subscription is independent from the Bitdefender Mobile Security subscription, meaning you will be able to use it for its entire availability, regardless of the state of your security subscription. In case the Bitdefender Premium VPN subscription expires, but the one for Bitdefender Mobile Security 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.

> **Note**
> Bitdefender VPN also works as a standalone application on all supported operating systems, namely Windows, macOS, Android and iOS.

5.6. Scam Copilot

This feature is essentially an AI-powered chatbot trained by Bitdefender to detect various scams, phishing attempts, misinformation campaigns and phony websites.

To activate Scam Copilot:

1. Open the Bitdefender Mobile Security app. In the Dashboard panel, a card pertaining to Scam Copilot will be present. Tap **Activate**.

2. Enable accessibility to Bitdefender Mobile Security by tapping the **TURN ON** button.

3. **Allow** Notification permission.

Scam Copilot is now properly configured on your device.

You can the access the Scam Copilot dedicated tab. Here you will find:

❍ **Scam Detection Chatbot:** Ask the chatbot to review any messages you find suspicious.

❍ **Prevention Assistant:** Helps you learn more about scams to become proficient in spotting them.

❍ **Automatic Scan Detection** status and control panel.

❍ **SMS filtering**: Have your dangerous messages filtered straight in your messaging app.

5.6.1. Scam Alert

The Scam Alert feature takes preventive measures to the forefront, dealing with potentially dangerous situations before they even have a chance to become a problem, including malware threats. Scam Alert monitors all incoming SMS messages and Android notifications in real-time.

When a dangerous link arrives in a message on your phone, a warning will pop up on your screen. Bitdefender will offer two options. The first option is to dismiss the information. The second option is to **VIEW DETAILS**. This provides you with more information about the incident, as well as essential pieces of advice, such as:

❍ Don't open or forward the detected link.

❍ For texts, delete the message if possible.

❍ Block the sender if they're not a trusted contact.

❍ Uninstall the app that sends dangerous links in notifications.

> **i** **Note**
> Due to Android operating system limitations, Bitdefender cannot delete text messages, take any direct measures related to the SMS messages, or any other source of malicious notifications. If you ignore the Scam Alert warning and try to open the dangerous link, Bitdefender's Web Protection feature will automatically catch it, preventing your device from becoming infected.

Activating Scam Alert

To enable Scam Alert, you need to grant the Bitdefender Mobile Security app access to the SMS messages and the notification system:

1. Open the Bitdefender Mobile Security app installed on your Android phone or tablet.

2. In the Bitdefender app main screen, tap the **Scam Alert** option on the bottom navigation bar, then press **TURN ON**.

3. Tap the **ALLOW** button.

4. In the Notification Access list, toggle Bitdefender Security to the **ON** position.

5. Confirm the action by pressing **ALLOW**.

6. Return to the Scam Alert screen and press **ALLOW** to give Bitdefender the ability to scan incoming SMS messages.

Real-time Chat Protection

Chat messages are our most comfortable mean of keeping in touch, but they're also an easy way for dangerous links to reach you.

With the Chat Protection feature active, the Scam Alert module is extended from protecting your texts and notifications to keeping your chats safe against link-based attacks as well, by detecting dangerous links your either send or receive while chatting.

To enable Chat Protection:

1. Open the Bitdefender Mobile Security app installed on your Android phone or tablet.

2. In the Bitdefender app main screen, tap the **Scam Alert** option on the bottom navigation bar.

3. You will be met by the Chat Protection feature at the top of the Scam Alert tab. Toggle its corresponding switch to the **ON** position.

> ⓘ **Note**
> Currently, Chat Protection is compatible with the following applications:
> ❍ WhatsApp
> ❍ Facebook Messenger
> ❍ Telegram
> ❍ Discord

5.7. Anti-Theft Features

Bitdefender can help you locate your device and prevent your personal data from getting into the wrong hands.

All you need to do is activate Anti-Theft from the device and, when needed, access **Bitdefender Central** from any web browser, anywhere.

> ⓘ **Note**
> The Anti-Theft interface also includes a link to our Bitdefender Central app on Google Play Store. You can use this link to download the app, in case you haven't done it already.

Bitdefender Mobile Security offers the following Anti-Theft features:

Remote Locate

View your device's current location on Google Maps. The location is refreshed every 5 seconds, so you can track it if it is on the move.

The accuracy of the location depends on how Bitdefender is able to determine it:

❍ If the GPS is enabled on the device, its location can be pinpointed to within a couple of meters as long it is in the range of GPS satellites (i.e. not inside a building).

❍ If the device is indoors, its location can be determined to within tens of meters if Wi-Fi is enabled and there are wireless networks available in its range.

❍ Otherwise, the location will be determined using only information from the mobile network, which can offer an accuracy no better than several hundred meters.

Remote Lock

Lock your device's screen and set a numeric PIN for unlocking it.

Remote Wipe

Remove all personal data from your estranged device.

Send alert to device (Scream)

Remotely send a message to be displayed on the device's screen, or trigger a loud sound to be played on the device speaker.

If you lose your device, you can let whoever finds it know how they can return it to you by displaying a message on the screen of the device.

If you misplaced your device and there is a chance it is not far from you (for example, somewhere around the house or the office), what better way to find it than to make it play a loud sound? The sound will be played even if the device is in silent mode.

5.7.1. Activating Anti-Theft

To enable Anti-Theft features, simply complete the configuration process from the Anti-Theft card available in the Dashboard.

Alternatively, you can activate Anti-Theft by following these steps:

1. Tap ⁘ **More** on the bottom navigation bar.

2. Tap ⊚ **Anti-Theft**.

3. Tap **TURN ON**.

4. The following procedure will begin to help you activate this feature:

    > (i) Note
    > Additional permissions are required on Android 6 for the Anti-Theft feature.
    >
    > To enable it, follow these steps:
    >
    > a. Tap **Activate Anti-Theft**, then tap **TURN ON**.
    >
    > b. Allow permissions for **Antivirus** to access your device's location.

    a. **Grant Admin Privileges**

These privileges are essential to the operation of Anti-Theft and therefore must be granted to continue.

b. **Set Application PIN**

To prevent unauthorized access to your device, a PIN code must be set. Every time an attempt will be made to access your device, the PIN will have to be entered first. Alternatively, on devices that support fingerprint authentication, a fingerprint confirmation can be used instead of the configured PIN code.

The same PIN code is used by App Lock to protect your installed apps.

c. **Activate Snap Photo**

Each time someone will try to unlock your device without success while Snap Photo is turned on, Bitdefender will take a photo of him.

More exactly, every time the PIN code, password, or fingerprint confirmation you set to protect your device is entered wrong three times in a row, a photo is taken using the front camera. The photo is saved together with the time-stamp and reason, and can be seen when you open Bitdefender Mobile Security and access the Anti-Theft window.

Alternatively, you can view the taken photo in your Bitdefender account:

i. Go to: https://central.bitdefender.com.

ii. Sign in to your account.

iii. Select the **My Devices** panel.

iv. Select your Android device, and then the **Anti-Theft** tab.

v. Tap ⋮ next to **Check your snapshots** to view the latest photos that were taken.
Only the two most recent photos are saved.

Once the Anti-Theft feature is activated, you can enable or disable Web Control commands individually from the Anti-Theft window by tapping the corresponding options.

5.7.2. Using Anti-Theft features from Bitdefender Central

> **(i) Note**
> All Anti-Theft features require the **Background data** option to be enabled in your device's Data usage settings.

To access the Anti-Theft features from your Bitdefender account:

1. Access Bitdefender Central.

2. Select the **My Devices** panel.

3. In the **MY DEVICES** window, select the desired device card by tapping on its corresponding **View details** button.

4. Select the **Anti-Theft** tab.

5. Tap the button corresponding to the feature you want to use:
   Locate - display your device's location on Google Maps.
   SHOW IP - displays the last IP address for the selected device.
   Alert - type a message to display on your device's screen and/or make your device play a sound alarm.
   Lock - lock your device and set a PIN code for unlocking it.
   Wipe - delete all data from your device.

> **(!) Important**
> After you wipe a device, all Anti-Theft features cease to function.

5.7.3. Anti-Theft Settings

If you wish to enable or disable the remote commands:

1. Tap **More** on the bottom navigation bar.

2. Tap **Anti-Theft**.

3. Enable or disable the desired options.

5.8. Account Privacy

Bitdefender Account Privacy detects if any data breach has occurred in the accounts you use for making online payments, shopping, or signing in different apps or websites. The data that may be stored into an account can be passwords, credit card information, or bank account information,

and, if not properly secured, identity theft or invasion to privacy may occur.

The privacy status of an account is displayed right after validation.

Automatic rechecks are set to run in the background, but manual scans can be run as well on a daily basis.

Notifications will be displayed each time new breaches that include any of the validated email accounts are discovered.

To start keeping personal information safe:

1. Tap ⠶ **More** on the bottom navigation bar.

2. Tap ◉ **Account Privacy**.

3. Tap **GET STARTED**.

4. The email address used to create your Bitdefender account appears and is automatically added to the list of monitored accounts.

5. To add another account, tap **ADD ACCOUNT** in the Account Privacy window, and then type the e-mail address.
   Tap **ADD** to continue.
   Bitdefender needs to validate this account before displaying private information. Therefore, an email with a validation code is sent to the provided email address.
   Check your inbox, and then type the received code in the **Account Privacy** area of your app. If you cannot find the validation email in the Inbox folder, check the Spam folder.
   The privacy status of the validated account is displayed.

If breaches are found in any of your accounts, we recommend you to change their password as soon as possible. To create a strong and secure password, take into consideration these tips:

❍ Make it at least eight characters long.

❍ Include lower and upper case characters.

❍ Add at least one number or symbol, such as #, @, % or !.

Once you secured an account that was part of a privacy breach, you can confirm the changes by marking the identified breach(es) as Solved. To do this:

1. Tap ⠶ **More** on the bottom navigation bar.

2. Tap ◎ **Account Privacy**.

3. Tap the account you just secured.

4. Tap the breach you secured the account for.

5. Tap **SOLVED** to acknowledge that the account is secured.

When all the detected breaches are marked as **Solved**, the account will no longer appear as breached, at least until a new breach is detected.

To stop being notified each time automatic scans are done:

1. Tap ⠶ **More** on the bottom navigation bar.

2. Tap ✿ **Settings**.

3. Turn off the corresponding switch in the Account Privacy area.

5.9. App Lock

Installed apps such as emails, photos, or messages, can contain personal data that you would like to remain private by selectively restricting access to them.

App Lock helps you block unwanted access to apps by setting a security PIN access code. The PIN code you set must be at least 4 digits long, but not more than 8, and is required every time you want to access the selected restricted apps.

Biometric authentication (such as fingerprint confirmation or face recognition) can be used instead of the configured PIN code.

5.9.1. Activating App Lock

To restrict access to selected apps, configure App Lock from the card displayed in the Dashboard after activating Anti-Theft.

Alternatively, you can activate App Lock by following these steps:

1. Tap ⠶ **More** on the bottom navigation bar.

2. Tap ◎ **App Lock**.

3. Tap **TURN ON**.

4. Allow access to usage data for Bitdefender Security.

5. Allow **draw over other apps**.

6. Go back to the app, configure the access code, and then tap **SET PIN**.

> **i** Note
> This step is available only if you didn't previously configure the PIN in Anti-Theft.

7. Enable the Snap Photo option to catch any intruder that will try to access your private data.

> **i** Note
> Additional permissions are required on Android 6 for the Snap Photo feature. To enable it, allow **Antivirus** to take pictures and record video.

8. Select the apps you want to protect.

Using the wrong PIN or fingerprint five times in a row, will activate a 30 seconds time-out session. This way, any attempt to break in the protected apps will be blocked.

> **i** Note
> The same PIN code is used by Anti-Theft to help you locate your device.

Set Application PIN

Set an application PIN to prevent unauthorized access to your device and apps. Also used by Anti-Theft.

Enter PIN (4–8 digits)

NOT NOW   SET PIN

5.9.2. Lock mode

The first time you add an app to App Lock, the App Lock Mode screen appears. From here you can choose when the App Lock feature should protect the apps installed on your device.

You can choose from one of the following options:

❍ **Require unlock every time** - each time the locked apps are accessed, the PIN code or fingerprint you have set up will have to be used.

❍ **Keep unlocked until screen off** - the access to your apps will be valid until the screen turns off.

❍ **Lock after 30 seconds** - you can exit and access again your unlocked apps within 30 seconds.

If you would like to change the selected setting:

1. Tap ∴ **More** on the bottom navigation bar.

2. Tap ✿ **Settings**.

3. Tap **Require unlock every time** in the App Lock area.

4. Choose the desired option.

5.9.3. App Lock Settings

For an advanced configuration of App Lock:

1. Tap ∴ **More** on the bottom navigation bar.

2. Tap ✿ **Settings**.

In the App Lock area, you can configure the following options:

❍ **Sensitive app suggestion** - receive a lock notification each time you are installing a sensitive app.

❍ **Require unlock every time** - choose one of the available lock and unlock options.

❍ **Smart Unlock** - keep apps unlocked while you are connected to trusted Wi-Fi networks.

❍ **Random keyboard** - prevent PIN reading by randomizing number positions.

5.9.4. Snap Photo

With Bitdefender Snap Photo you can catch your friends or relatives on the hop. This way you can educate their curious eyes to not look through your personal files or the apps you use.

The feature works easy: each time the PIN code or fingerprint confirmation you set to protect your apps is entered wrong three times in a row, a photo is taken using the front camera. The photo is saved together with the time-stamp and reason, and can be seen when you open Bitdefender Mobile Security and access the App Lock feature.

> **Note**
> This feature is available only for phones that have a front camera.

To configure the Snap Photo feature for App Lock:

1. Tap ⁘ **More** on the bottom navigation bar.
2. Tap ✿ **Settings**.
3. Enable the corresponding switch in the Snap Photo area.

The photos snapped when the incorrect PIN is entered are displayed in the App Lock window and can be viewed full-screen.

Alternatively, they can be viewed in your Bitdefender account:

1. Go to: https://central.bitdefender.com.
2. Sign in to your account.
3. Select the **My Device** panel.
4. Select your Android device, and then the **Anti-Theft** tab.
5. Tap ⋮ next to **Check your snapshots** to view the latest photos that were taken.

Only the two most recent photos are saved.

To stop uploading snapped photos on your Bitdefender account:

1. Tap ⁘ **More** on the bottom navigation bar.
2. Tap ✿ **Settings**.
3. Disable **Upload photos** in the Snap Photo area.

5.9.5. Smart Unlock

An easy method to stop being asked by the App Lock feature to enter the PIN code or fingerprint confirmation for the protected apps each time you access them is to activate Smart Unlock.

With Smart Unlock you can set as trusted the Wi-Fi networks you usually connect to, and when connected to them, the App Lock blocking settings will be disabled for the protected apps.

To configure the Smart Unlock feature:

1. Tap ⁚• **More** on the bottom navigation bar.

2. Tap ⓡ **App Lock**.

3. Tap the ♥ button.

4. Tap the switch next to **Smart Unlock**, if the feature is not yet enabled. Validate using your fingerprint or your PIN.
The first time you'll activate the feature, you will need to enable the location permission. Tap the **ALLOW** button, then tap **ALLOW** again.

5. Tap **ADD** to set the Wi-Fi connection you're currently using as trusted.

Whenever you change your mind, disable the feature and the Wi-Fi networks you have set as trusted will be treated as untrusted.

5.10. Reports

The Reports feature keeps a detailed log of events concerning the scanning activity on your device.

Whenever something relevant to the security of your device happens, a new message is added to the Reports.

To access the Reports section:

1. Tap ⁚• **More** on the bottom navigation bar.

2. Tap 🦋 **Reports**.

The following tabs are available in the Reports window:

❍ **WEEKLY REPORTS** - here you have access to the security status and the performed tasks from the current and previous week. The current week's report is generated each Sunday and you will receive a notification informing you about it becoming available.
Each week a new tip will be displayed in this section, so make sure you check back regularly to get the best out of the app.
To stop receiving notifications each time a report is generated:

1. Tap ⁙ **More** on the bottom navigation bar.

2. Tap ✿ **Settings**.

3. Disable the **New report notification** switch in the Reports area.

❍ **ACTIVITY LOG** - here you can check detailed information about the activity of your Bitdefender Mobile Security app since it was installed on your Android device.
To delete the available activity log:

1. Tap ⁙ **More** on the bottom navigation bar.

2. Tap ✿ **Settings**.

3. Tap **Clear Activity Log**, and then tap **CLEAR**.

5.11. WearON

With Bitdefender WearON you can easily find your smartphone whether you left it at the office in a conference room or under a pillow on your couch. The device can be found even if the silent mode is activated.

Keep this feature enabled to make sure that you always have your smartphone at hand.

ⓘ Note
The feature works with Android 4.3 and Android Wear.

5.11.1. Activating WearON

To use WearON, you only have to connect your smartwatch to the Bitdefender Mobile Security app and activate the feature with the following voice command:

Start:<Where is my phone>

Bitdefender WearON has two commands:

1. **Phone Alert**
With the Phone Alert feature you can quickly find your smartphone whenever you step too far away from it.
If you have your smartwatch with you, it automatically detects the app on your phone and vibrates whenever you go too far from your phone, more exactly when the Bluetooth connectivity is lost.

To enable this feature, open Bitdefender Mobile Security, tap **Global Settings** in the menu and select the corresponding switch under the WearON section.

2. **Scream**

Finding your phone has never been easier. Whenever you forget where you left your phone, tap the Scream command on your watch to make your phone scream.

5.12. About

To find information about the Bitdefender Mobile Security version you have installed, to access and read the Subscription Agreement and Privacy Policy, and view the Open-source licenses:

1. Tap ⁙ **More** on the bottom navigation bar.

2. Tap ⚙ **Settings**.

3. Tap the desired option in the About area.

5.13. Frequently Asked Questions

Why does Bitdefender Mobile Security require an internet connection?

The app needs to communicate with Bitdefender servers to determine the security status of the apps it scans and of the webpages you are visiting, and also to receive commands from your Bitdefender account, when using the Anti-Theft features.

What does Bitdefender Mobile Security need each permission for?

❍ Internet access -> used for cloud communication.

❍ Read phone state and identity -> used to detect if the device is connected to the internet and to extract certain device info needed to create a unique ID when communicating to Bitdefender cloud.

❍ Read and write browser bookmarks -> Web Protection module deletes malicious sites from your browsing history.

❍ Read log data -> Bitdefender Mobile Security detects traces of threat activities from the Android logs.

❍ Location -> required for remote location.

❍ Camera -> required for Snap photo.

❍ Storage -> used to allow the Malware Scanner to check the SD card.

How can I stop submitting to Bitdefender information about suspect apps?

By default, Bitdefender Mobile Security sends reports to Bitdefender servers about the suspect apps you are installing. This information is essential for improving the threat detection and can help us to offer you a better experience in the future. In case you want to stop sending us information about suspect apps:

1. Tap ⁘ **More** on the bottom navigation bar.

2. Tap ✿ **Settings**.

3. Turn off **In-the-cloud detection** in the Malware Scanner area.

Where can I see details about the app's activity?

Bitdefender Mobile Security keeps a log of all important actions, status changes, and other critical messages related to its activity. To access see about the app's activity:

1. Tap ⁘ **More** on the bottom navigation bar.

2. Tap ⩔ **Reports**.
   In the WEEKLY REPORTS window you can access the reports that are generated every week and in the ACTIVITY LOG window you can view information about the activity of your Bitdefender app.

I forgot the PIN code that I set to protect my app. What do I do?

1. Access Bitdefender Central.

2. Select the **My Devices** panel.

3. Tap the desired device card, and then tap ⋮ in the upper-right corner of the screen.

4. Select **Settings**.

5. Retrieve the PIN code from the **Application PIN** field.

How can I change the PIN code I set for App Lock and Anti-Theft?

If you wish to change the PIN code you set for App Lock and Anti-Theft:

1. Tap ⁘ **More** on the bottom navigation bar.

2. Tap ✿ **Settings**.

3. Tap Security **PIN CODE** in the Anti-Theft area.

4. Type in the current PIN code.

5. Type in the new PIN code you want to set.

How can I switch off the App Lock feature?

There is no turn off option for the App Lock feature, but you can easily disable it by clearing the check boxes next to the selected apps after validating the PIN or fingerprint you have set.

How can I set another wireless network as trusted?

First, you have to connect your device to the wireless network you want to set as trusted. Then follow these steps:

1. Tap ⁛ **More** on the bottom navigation bar.

2. Tap ⊚ **App Lock**.

3. Tap 🛡 in the upper-right corner.

4. Tap **ADD** next to the network you want to set as trusted.

How can I stop seeing snapped photos taken on my devices?

To stop making visible the snapped photos taken on your devices:

1. Access Bitdefender Central.

2. Tap 🖳 in the upper right side of the screen.

3. Tap **Settings** in the slide menu.

4. Disable the **Show/don't show snap photos taken on your devices** option.

How can I keep my online shopping secure?

Online shopping comes with high risks when some details are ignored. To not become a victim of fraud, we recommend you the following:

❍ Keep your security app updated.

❍ Submit online payments only with buyer protection.

❍ Use a VPN when connecting to the internet from public and unsecured wireless networks.

❍ Pay attention to the passwords you have assigned to your online accounts. They have to be strong including capital and lowercase letters, numbers and symbols (@, !, %, #, etc.).

❍ Make sure that the information you send is over secure connections. The online website extension has to be HTTPS://, and not HTTP://.

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 you are home or abroad

❍ want 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.

Can I change the Bitdefender account linked to my device?

Yes, you can easily change the Bitdefender account linked to your device by following these steps:

1. Tap ⁘ **More** on the bottom navigation bar.

2. Tap your email address.

3. Tap **Log out of your account**. If a PIN code has been set, you are prompted to type it.

4. Confirm your choice.

5. Type the email address and the password of your account in the corresponding fields, and then tap **SIGN IN**.

How will Bitdefender Mobile Security impact my device's performance and battery autonomy?

We keep the impact very low. The app only runs when it is essential - after you install an app, when you browse the app interface or when you want a security check. Bitdefender Mobile Security does not run in the background when you call your buddies, type a message or play a game.

What is Device Administrator?

Device Administrator is an Android feature that gives Bitdefender Mobile Security the permissions needed to perform certain tasks remotely. Without these privileges, remote lock would not work and device wipe would not be able to completely remove your data. If you want to remove the app, make sure to revoke these privileges before trying to uninstall from **Settings > Security > Select device administrators**.

How to fix "No Google Token" error that appears when signing in to Bitdefender Mobile Security.

This error occurs when the device is not associated with a Google account, or the device is associated with an account but a temporary problem is preventing it from connecting to Google. Try one of the following solutions:

❍ Go to Android Settings > Applications > Manage Applications > Bitdefender Mobile Security and tap **Clear data**. Then try to sign in again.

❍ Make sure your device is associated with a Google account.
   To check this, go to Settings > Accounts & sync and see if a Google account is listed under **Manage Accounts**. Add your account if one is not listed, restart your device and then try to sign in to Bitdefender Mobile Security.

❍ Restart your device, and then try to sign in again.

In what languages is Bitdefender Mobile Security available?

Bitdefender Mobile Security is currently available in the following languages:

- ❍ Brazilian
- ❍ Czech
- ❍ Dutch
- ❍ English
- ❍ French
- ❍ German
- ❍ Greek
- ❍ Hungarian
- ❍ Italian
- ❍ Japanese
- ❍ Korean
- ❍ Polish
- ❍ Portuguese
- ❍ Romanian
- ❍ Russian
- ❍ Spanish
- ❍ Swedish
- ❍ Thai
- ❍ Turkish
- ❍ Vietnamese

Other languages will be added in future releases. To change the language of the Bitdefender Mobile Security interface, go to your device's **Language & keyboard** settings and set the device to the language you want to use.

6. MOBILE SECURITY FOR IOS

6.1. What is Bitdefender Mobile Security for iOS

Online activities such as paying bills, making holiday reservations, or buying goods and services are convenient and hassle-free. But as many activities evolved on the internet, these come with high risks and, if security details are ignored, personal data may be hacked. And what is more important than protecting data stored in online accounts and on the personal smartphone?

Bitdefender Mobile Security for iOS allows you to:

❍ Gain the most powerful protection against threats with the least impact on battery

❍ Protect your personal data: passwords, address, social and financial information

❍ Easily check your phone security to detect and fix misconfigurations that might expose it

❍ Avoid accidental data exposure and misuse for all installed apps

❍ Scan your device to achieve optimal security and privacy settings

❍ Gain usage insights into your online activity and history of prevented incidents

❍ Check your online accounts against data breaches or data leaks

❍ Encrypt internet traffic with the included VPN

Bitdefender Mobile Security for iOS is delivered free of charge and requires activation with a Bitdefender account. However, some important features of Bitdefender, such as our 'Web Protection' module, require a paid subscription in order to be accessible to our users.

6.2. Getting Started

6.2.1. Device Requirements

Bitdefender Mobile Security for iOS works on any device running iOS 12 or later versions of the operating system and needs an active internet

connection to be activated and to detect if any data leakage has occurred in your online accounts.

6.2.2. Installing Bitdefender Mobile Security for iOS

❍ **From Bitdefender Central**

  ❍ On iOS

  1. Access Bitdefender Central.

  2. Select the **My Devices** panel.

  3. Tap **INSTALL PROTECTION**, and then tap **Protect this device**.

  4. Select the owner of the device. If the device belongs to someone else, tap the corresponding button.

  5. You are redirected to the **App Store** app. In the App Store screen, tap the installation option.

  ❍ On Windows, macOS, Android

  1. Access Bitdefender Central.

  2. Select the **My Devices** panel.

  3. Press **INSTALL PROTECTION**, and then press **Protect other devices**.

  4. Select the owner of the device. If the device belongs to someone else, press the corresponding button.

  5. Press **SEND DOWNLOAD LINK**.

  6. Type an email address in the corresponding field, and press **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.

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

❍ **From App Store**
Search for Bitdefender Mobile Security for iOS to locate and install the app.

An introduction window containing details about the product features is displayed the first time you open the app. Tap Get started to proceed to the next window.

Before going through the validation steps, 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 Mobile Security for iOS.

Tap **Continue** to proceed to the next window.

6.2.3. Sign in to your Bitdefender account

To use Bitdefender Mobile Security for iOS you must link your device to a Bitdefender, Facebook, Google, Apple, or Microsoft account by signing in to the account from the app. The first time you open the app, you are be prompted to sign in to an account.

To link your device to a Bitdefender account:

1. Type your Bitdefender account email address in the corresponding field, and then tap **NEXT**. If you do not have a Bitdefender account and want to create one, select the corresponding link, and then follow the onscreen instructions until the account is activated.
   To sign in using a Facebook, Google, Apple, or Microsoft account, tap the service you want to use from the **Or sign in** with area. You are redirected to the sign in page of the selected service. Follow the instructions to link your account to Bitdefender Mobile Security for iOS.

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

2. Type your password, and then tap **SIGN IN**.

From here you can also access the Bitdefender Privacy Policy.

6.2.4. Dashboard

Tap the Bitdefender Mobile Security for iOS icon in your device's app drawer to open the application interface.

The first time you access the app, you are prompted to allow Bitdefender to send you notifications. Tap **Allow** to stay informed each time Bitdefender has to communicate you something relevant to your app. To manage Bitdefender notifications, go to Settings > Notifications > Mobile Security.

To get access to the section you need, tap the corresponding icon from the bottom of the screen.

Web Protection

Stay safe while you surf the web and whenever less secure apps will try to access untrusted domains. For more information, refer to Web Protection (page 212).

VPN

Maintain your privacy no matter what network you are connected to by keeping your internet communication encrypted. For more information, refer to VPN (page 214).

Account Privacy

Find out whether your email accounts have been leaked or not. For more information, refer to Account Privacy (page 217).

To see additional options, tap the ••• icon on your device while in the application's home screen. The following options appear:

❍ **Restore purchases** - from here you can restore the previous subscriptions you have purchased through your iTunes account.

❍ **Settings** - from here you have access to:

   ❍ **VPN Settings**

      ❍ **Agreement** - you can read the terms under which you use the Bitdefender VPN service. If you tap **I don't agree anymore**, you will not be able to use Bitdefender VPN at least until you tap **I Agree**.

      ❍ **Open Wi-Fi warning** - you can enable or disable the product notification that appears each time you connect to an unsecured Wi-Fi network.
      The purpose of this notification is to help you keep your data private and secure by using Bitdefender VPN.

❍ **Web Protection Settings**

  ❍ **Agreement** - you can read the terms under which you use the Bitdefender Web Protection service. If you tap **I don't agree anymore**, you will not be able to use Bitdefender VPN at least until you tap **I Agree**.

  ❍ **Enable Web Protection notification** - Notifies you that Web Protection can be enabled after finishing a VPN session.

  ❍ **Product reports**

❍ **Feedback** - from here you can launch the default email client to send us your feedback about the app.

❍ **App info** - from here, you have access to information about the installed version and to Subscription Agreement, Privacy Policy, and Open-source licenses compliances.

6.3. Scan

Bitdefender Mobile Security for iOS allows you to scan your device for any security vulnerabilities and potential threats on your device. Running the scan will check for:

❍ **OS version:** Checking your iOS version for the latest updates.

❍ **Passcode/Biometrics:** Checking the security level in regards to accessing your device.

❍ **Web Protection:** Checking the state of the Web Protection module

❍ **Account Privacy:** Checking for the presence of monitored accounts listed in the Account Privacy module.

❍ **Scan Wi-Fi:** Checking for the security status of the currently connected network.

The protection status is determined after you run a manual scan.

After running the first scan, you will be met with Bitdefender's Autopilot recommendations. This is your personal security advisor, providing contextual recommendations based on your device usage and needs. This way, you'll get to benefit from everything your app has to offer.

> **Note**
> When first entering the app, you will be prompted to run a scan.

6.4. Scam Copilot

This feature is essentially an AI-powered chatbot trained by Bitdefender to detect various scams, phishing attempts, misinformation campaigns and phony websites.

To activate Scam Copilot:

1. Open the Bitdefender Mobile Security app. In the Dashboard panel, a card pertaining to Scam Copilot will be present. Tap **Activate**.
2. You will have to enable SMS filtering as instructed below:
   a. Open **Settings** on your device.
   b. Select **Messages** from the list.
   c. Select **Unknown and Spam**.
   d. Toggle ON **Filter Unknown Senders**.
   e. Select **Mobile Security** in SMS Filtering.
3. Once you are finished, press **Continue**.
4. Enable Calendar scan. A pop-up will appear on your screen shortly after pressing the **Enable** button. Tap on **Allow Full Access**.

Scam Copilot is now properly configured on your device.

You can the access the Scam Copilot dedicated tab. Here you will find:

❍ **Scam Detection Chatbot:** Ask the chatbot to review any messages you find suspicious.
❍ **Prevention Assistant:** Helps you learn more about scams to become proficient in spotting them.
❍ **Automatic Scan Detection** status and control panel.
❍ **SMS filtering**: Have your dangerous messages filtered straight in your messaging app.

6.4.1. Scam Alert

The Scam Alert feature available in Bitdefender Mobile Security for iOS proactively protects Apple users from phishing scams. Scam Alert for iOS

includes two layers of protection that monitor scams delivered through SMS/MMS messages and calendar invites:

❍ **Text Message Filter (SMS, MMS)**
This feature identifies and filters unwanted SMS and MMS messages.
A malicious SMS/MMS (Short Message Service/Multimedia Messaging Service) refers to a type of message sent to mobile devices with harmful intent. These messages are designed to exploit vulnerabilities, deceive recipients, or cause harm to the target's device, personal information, or security.

❍ **Calendar Invite Link Scanner**
This feature detects spam calendars and events that contain dangerous links. The calendar virus is a type of spam that affects the Calendar app of your iPhone, which can be annoying and potentially dangerous:

  ❍ You get unwanted calendar invitations or event notifications when you accidentally accept a fake calendar invite sent to your email address by hackers or spammers.

  ❍ When you click on the link in the invite, you unknowingly subscribe to the sender's calendar, which allows them to send you more spam events.

  ❍ The spam events may contain links or attachments that could lead you to phishing pages or other cyber-threats if you open them.

How to set up Scam Alert

To enable Scam Alert, you need to grant the Bitdefender Mobile Security app access to calendar notifications and SMS messages:

How to enable SMS Filtering:

In order for Bitdefender to start filtering messages, you must manually activate the Filter Unknown Senders option in Messages app settings:

1. Open the **Settings** app on your iPhone or iPad.

2. Scroll down and select **Messages** in the list.

3. Tap the **Unknown & Spam** section.

4. Toggle **Filter Unknown Senders** to the on position.

5. Select **Mobile Security** in the SMS Filtering section and then choose **Enable**.

Bitdefender will now be able to filter junk messages on your iPhone/iPad.

> **ⓘ Note**
> Due to iOS restrictions, Bitdefender SMS filtering can only be used for SMS and MMS messages that come from people you don't have saved in your contacts. This means it won't filter messages from people already in your contacts list or iMessage messages from anyone.

How to enable Calendar Scan:

1. Open the **Bitdefender Mobile Security** app installed on your iPhone or iPad.

2. Go to the **Scam Alert** option in the bottom navigation bar and press **Set up now**.

3. Tap **Continue**, and then tap **Enable**.

4. Choose **OK** to grant Bitdefender access to your calendar. A calendar scan will begin immediately.

6.5. Web Protection

Bitdefender Web Protection ensures a safe browsing experience by alerting you about potential malicious webpages and when less secure installed apps will try to access untrusted domains.

When an URL points to a known phishing or fraudulent website, or to malicious content such as spyware or viruses, the webpage is blocked and an alert is shown. The same thing happens when installed apps try to access malicious domains.

> **⚠ Important**
> If you are located in an area where the usage of a VPN service is restricted by law, the functionality of Web Protection will not be available.

To activate Web Protection:

1. Tap the 🌐 icon from the bottom of the screen.

2. Tap **I Agree**.

3. Enable the Web Protection switch.

> **i** Note
> The first time you turn on Web Protection, you might be prompted to allow Bitdefender to set up VPN configurations that will monitor network traffic. Tap **Allow**, to continue. If an authentication method (fingerprint or PIN code) has been set to protect your smartphone, you are required to use it. To be able to detect access to untrusted domains, Web Protection is working together with the VPN services.

> **!** Important
> The Web Protection feature and the VPN cannot function at the same time. Whenever one of them is enabled, the other (if it is active at that time) will be disabled.

6.5.1. Bitdefender alerts

Whenever you try to visit a website classified as unsafe, the website is blocked. To make you aware of the event, you are notified by Bitdefender in the Notification center and in your browser. The warning page contains information such as the website URL and the detected threat. You have to decide what to do next.

Also, you are notified in the Notification Center whenever a less secure app tries to access untrusted domains. Tap the displayed notification to be redirected to the window where you can decide what to do next.

The following options are available for both cases:

❍ Navigate away from the website by tapping **TAKE ME BACK TO SAFETY**.

❍ Proceed to the website, despite the warning, by tapping the displayed notification, and then **I want to access the page**.

Confirm your choice.

6.6. 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 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 Password Manager, you are able to access content that is normally restricted in specific areas.

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

To turn on Bitdefender VPN:

1. Tap the ⬡ icon from the bottom of the screen.

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

> **i** **Note**
> The first time you turn on VPN, you are prompted to allow Bitdefender to set up VPN configurations that will monitor network traffic. Tap **Allow**, to continue. If an authentication method (fingerprint or PIN code) has been set to protect your smartphone, you are required to use it.

The 🆅🅿🅽 icon appears in the status bar when VPN is active.

To save battery power, we recommend you to turn off VPN when you do not need it.

If you have a premium subscription and would like to connect to a server at your will, tap Automatic in the VPN interface, and then select the location you want. For details about VPN subscriptions, refer to Subscriptions (page 216).
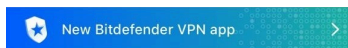
6.6.1. Subscriptions

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

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

You can upgrade to the Bitdefender Premium VPN version anytime by tapping the **Activate Premium VPN** button available in the VPN window. There are two types of subscriptions to choose from: annual and monthly.

The Bitdefender Premium VPN subscription is independent from the Bitdefender Mobile Security for iOS free subscription, meaning you will be able to use it for its entire availability. In case the Bitdefender Premium VPN subscription expires, your will be automatically 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.

> **i** Note
> Bitdefender VPN also works as a standalone application on all supported operating systems, namely Windows, macOS, Android and iOS.

6.7. Account Privacy

Bitdefender Account Privacy detects if any data leakage has occurred in the accounts you use for making online payments, shopping, or signing in different apps or websites. The data that may be stored into an account can be passwords, credit card information, or bank account information, and, if not properly secured, identity theft or invasion to privacy may occur.

The privacy status of an account is displayed right after validation.

To check if any of accounts has been leaked, tap **Scan for leaks**.

To start keeping personal information safe:

1. Tap the ◉ icon from the bottom of the screen.

2. Tap **Add account**.

3. Type your email address in the corresponding field, and then tap **Next**. Bitdefender needs to validate this account before displaying private information. Therefore, an email with a validation code is sent to the provided email address.

4. Check your inbox, and then type the received code in the **Account Privacy** area of your app. If you cannot find the validation email in the Inbox folder, check the Spam folder too.
   The privacy status of the validated account is displayed.

If leaks are found in any of your accounts, we recommend you to change their password as soon as possible. To create a strong and secure password, take into consideration these tips:

❍ Make it at least eight characters long.

❍ Include lower and upper case characters.

❍ Add at least one number or symbol, such as #, @, % or !.

Once you secured an account that was part of a privacy breach, you can confirm the changes by marking the identified leak(s) as **Solved**. To do this:

1. Tap ⋯ next to the breach you solved.

2. Tap **Mark as solved**.

When all the detected leaks are marked as Solved, the account will no longer appear as leaked, at least until a new leakage is detected.

6.8. Frequently Asked Questions

How does Bitdefender Mobile Security for iOS protect me against viruses and cyber threats?

Bitdefender Mobile Security for iOS provides absolute protection against all cyber threats and is especially designed to keep your sensitive data safe from prying eyes.

You get a wealth of advanced security and privacy features for your iPhone and iPad - plus many bonus features, including VPN and Web Protection.

Bitdefender Mobile Security for iOS reacts instantly to viruses and malware with no compromise to your system's performance.

What type of devices and operating systems does Bitdefender Mobile Security for iOS cover?

Bitdefender Mobile Security for iOS will protect your smartphones and tablets running iOS against all cyber threats.

Why do I need Bitdefender Mobile Security for iOS on Apple OS?

Some of your most personal data is stored on your iPhone or iPad - and you need to know it is safe at all times. Bitdefender Mobile Security for iOS provides absolute protection against cyber threats and takes care of your online privacy and private information without interfering in your day-to-day activities.

Do I get a VPN with my Bitdefender Mobile Security for iOS subscription?

Bitdefender Mobile Security for iOS comes with a basic version of Bitdefender VPN that includes a generous amount of traffic (200 MB/ day, a total of 6GB/ month) free of charge.

7. VPN

7.1. 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.

> (i) 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.

7.1.1. 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

> (i) 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.

7.2. Installation

7.2.1. 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 220)

❍ 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.

7.2.2. 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

7.2.3. 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**.

7.3. Using Bitdefender VPN

7.3.1. 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.

7.3.2. 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.
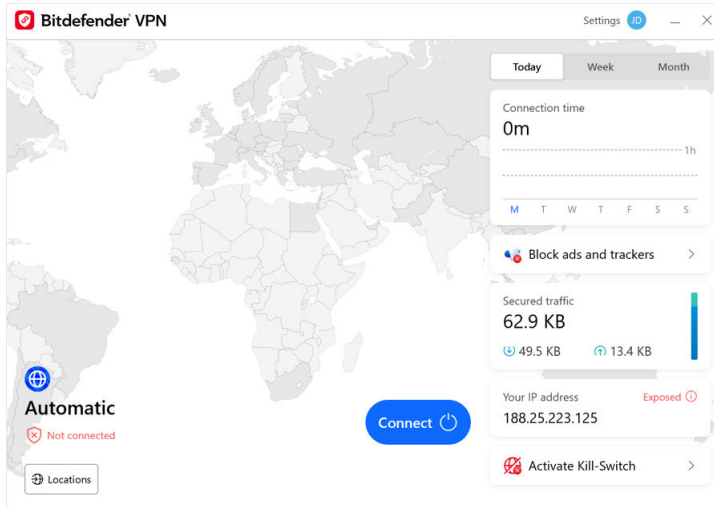
❍ **For Windows:** The system tray icon displays a green checkmark when the VPN is connected, and a black mark when the VPN is disconnected. While connected to a manually selected location, the IP address is displayed on the main interface.

❍ **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.

7.3.3. 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.

7.4. Bitdefender VPN Settings & Features

7.4.1. 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.

7.4.2. 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.

7.4.3. Features

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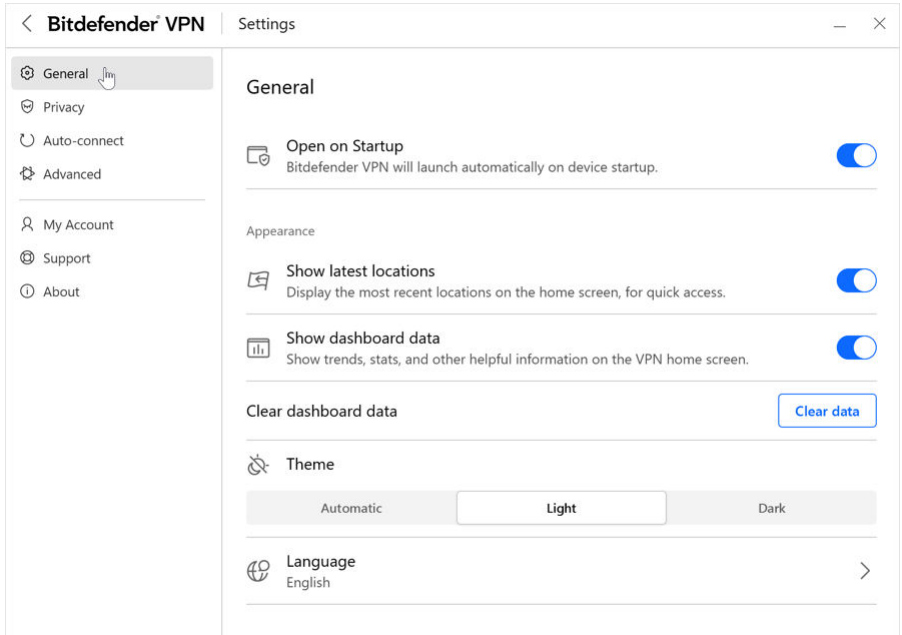
3. Under **Privacy**, enable the **Kill-Switch** option.

❍ **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.

> **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.

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.

> **ⓘ 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.

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**.

> **i** Note
> 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.

> **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.

7.5. 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**.

7.6. 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.

8. PASSWORD MANAGER

8.1. What is Bitdefender Password Manager

Bitdefender Password Manager is a multi-platform service designed to help users store and organize all of their online passwords. It is built with the strongest known cryptographic algorithms for the highest level of safety and digital security. It works as a browser extension and mobile app solution for identity and password management, banking and all other types of sensitive information across devices.

Bitdefender Password Manager can auto-save, auto-fill, automatically generate and manage your passwords for all websites and online services with the help of a single Master Password, making your overall digital identity much easier to manage.

8.1.1. Security and how it works

Behind the Bitdefender Password Manager software stand some of the latest cryptographic algorithms which assure the highest data security users can hope for, such as AES-256-CCM, SH512, BCRYPT, HTTPS and WSS protocols for data transmission. All data involved is at all times encrypted and decrypted locally. This makes it such that only the account holder alone can have access to the information stored within the account, as well as to the Master Password that is used to access and subsequently make use of the data in question.

8.2. Getting Started

8.2.1. System Requirements

You may use the latest version of Bitdefender Password Manager only on devices running the following operating systems:

❍ **For PC users:**

  ❍ Windows 7 with Service Pack 1

  ❍ Windows 8

  ❍ Windows 8.1

❍ Windows 10

❍ Windows 11

❍ **For macOS users:**

❍ macOS 10.14 (Mojave) and later macOS operating systems

> ⓘ **Note**
> Note that System Performance may be affected on devices that have old generation CPUs.

❍ **For iOS users:**

❍ iOS 11.0 or later iOS operating systems

❍ **For Android users:**

❍ Android 5.1 and later Android operating systems

> ⓘ **Note**
> ❍ Fingerprint unlock feature is supported on **Android 6.0** and later.
> ❍ Autofill feature is supported on **Android 8.0** and later, compatible with iPhone, iPad and iPod touch.

Software Requirements

To be able to use Bitdefender Password Manager and all its features, your Windows or macOS devices need to meet the following software requirements:

❍ **Microsoft Edge** (based on Chromium 80 and later)

❍ **Mozilla Firefox** (version 65 or later)

❍ **Google Chrome** (version 72 or later)

❍ **Safari** (version 12 or later)

> ⓘ **Note**
> The Sofware Requirements are not applicable for Android and iOS.

> ❌ **Warning**
> Failure to meet the System Requirements presented above will result in either the inability of installing Bitdefender Password Manager or the malfunctioning of the product.

8.2.2. Installation

This chapter will guide you on how to install Bitdefender Password Manager to both the web browsers on your Windows PC and macOS, as well as on your mobile Android or iOS devices.

> ⚠ Important
>
> Prior to the installation, make sure that you have a valid Password Manager subscription in your Bitdefender Central account so that this browser extension can retrieve its validity from your account.
>
> Active subscriptions are listed in the **My Subscriptions** section within Bitdefender Central.

Installing on Windows and macOS devices

Unlike most desktop applications and software which need to be installed and set up on these devices, Bitdefender Password Manager comes as a browser extension - also called an add-on - that can be quickly added and enabled to your preferred browser.

The currently supported browsers for the product are the following: **Google Chrom**e, **Mozilla Firefox**, **Microsoft Edge**, and **Safari**.

1. Go to https://central.bitdefender.com/ and sign in to your account.
   If you don't already have an account, click on **CREATE ACCOUNT**, then type your full name, an email address and a password.

2. Select **My Devices** on the left sidebar of the screen.

3. In the **My Devices** section, proceed by clicking on **+ Add Device**.

4. This action will prompt a new window to pop up. Choose **Password Manager** in the selection screen.

5. Choose **This Device**.
   If you are looking to install on a different device, select Other devices. You can then email a download link to the respective device or directly copy the URL for the installation.

6. Next choose on which browser you want to install the Password Manager extension.

7. Each corresponding button will redirect you to the browser's Extensions Store. From there, simply follow the instructions on screen as shown below:

Microsoft Edge

❍ Click the **Get** button

❍ Click **Add extension** in the prompt that appears on screen

Google Chrome

❍ Click the **Add to Chrome** button

❍ In the confirmation box, click **Add extension**

Mozilla Firefox

❍ Click the **Add to Firefox** button

❍ Click the **Install** button in the upper right corner of the screen

Safari

❍ Click the **Get** button, then click **Install**

❍ Open Safari and select **Preferences** in the top menu bar

❍ In the Preferences window, click the **Extensions** tab

❍ Select the checkbox next to Password Manager to enable it

Once you have followed these steps, set a strong master password, then press the **Save Master Password** button after you read and agree with the **Terms and conditions**.

> ⚠ **Important**
>
> Note that you will require this Master Password to unlock all the passwords, credit card information and notes saved in Bitdefender Password Manager. This is essentially the key that allows the owner to use this product.

> ❌ **Warning**
>
> Upon creating the Master Password, you will receive a **24-digit recovery key**. Make a note of your recovery key in a safe place and don't lose it. This key is the only way to access your passwords saved in Password Manager in the event that you happen to **forget the Master Password** previously set up for your account.

❍ You can press **Close** when done.

Installing on Android devices

The easiest method of installing Bitdefender Password Manager for Android phones and tablets is to download the application directly from Google Play.

Installing the Bitdefender Password Manager app can also be done through your Bitdefender Central account:

1. On your Android mobile device sign in to your Bitdefender Central account by accessing https://login.bitdefender.com/central/login.

2. Select **My Devices** on the left sidebar of the screen.

3. In the **My Devices** section, proceed by clicking on **+ Add Device**.

4. This action will prompt a new window to pop up. Choose **Password Manager** in the selection screen.

5. Choose **This Device**.
   If you are looking to install on a different device, select **Other devices**. You can then email a download link to the respective device or directly copy the URL for the installation.

6. You will be redirected to Google Play. Tap **Install** to download Bitdefender Password Manager on Android.

7. Once the download is completed, open the 🛡 Password Manager application.

8. If you are not automatically logged in to your account, sign in using your username and password.
   Once you have followed these steps, set a strong master password, then press the **Save Master Password** button after you read and agree with the **Terms and conditions**.

> ⚠ Important
> Note that you will require this Master Password to unlock all the passwords, credit card information and notes saved in Bitdefender Password Manager. This is essentially the key that allows the owner to use this product.

> ## ✖ Warning
>
> Upon creating the Master Password, you will receive a **24-digit recovery key**. Make a note of your recovery key in a safe place and don't lose it. This key is the only way to access your passwords saved in Password Manager in the event that you happen to **forget the Master Password** previously set up for your account.
>
> ❍ You can press **Close** when done.

9. Create a **4-digit PIN**, so if you switch to another app and then return to Password Manager, you won't have to re-enter the master password you set up previously. If available, you can also enable face recognition or fingerprint authentication.

10. Tap on **Enable Autofill** to configure Android autofill settings.

> ## ⓘ Note
>
> If you skip this step, you can enable and customize the Android autofill features at a later time by following the instructions available at Intelligent Autofill (page 254).

11. You will be met by a list of apps that can autofill passwords.
    · Select **Password Manager** and then the device will prompt you to confirm that you trust this app.
    Tap **OK**.

12. Enter the PIN you set up in **step 9** to confirm this action.

The installation on your Android device is now complete.

Installing on iOS devices

The easiest method of installing Bitdefender Password Manager for iOS and iPadOS devices is to download the application from the Apple App Store.

Installing the Bitdefender Password Manager app can also be done through your Bitdefender Central account:

1. On your iPhone or iPad sign in to your Bitdefender Central account by accessing https://login.bitdefender.com/central/login.

2. Select **My Devices** on the left sidebar of the screen.

3. In the **My Devices** section, proceed by clicking on **+ Add Device**.

4. This action will prompt a new window to pop up. Choose **Password Manager** in the selection screen.

5. Choose **This Device**.
   If you are looking to install on a different device, select **Other devices**. You can then email a download link to the respective device or directly copy the URL for the installation.

6. You will be redirected to **App Store**. Tap the cloud icon with an arrow pointing down to download Bitdefender Password Manager for iOS.

7. Once the 🛡️ application is installed, open it and check the small box on the screen. Select **Continue** after you read and agree with the **Subscription Agreement**.

8. If you are not automatically logged in to your account, sign in using your username and password.
   Once you have followed these steps, set a strong master password, then press the **Save Master Password** button after you read and agree with the **Terms and conditions**.

   ⚠️ Important
   Note that you will require this Master Password to unlock all the passwords, credit card information and notes saved in Bitdefender Password Manager. This is essentially the key that allows the owner to use this product.

   ❌ Warning
   Upon creating the Master Password, you will receive a **24-digit recovery key**. Make a note of your recovery key in a safe place and don't lose it. This key is the only way to access your passwords saved in Password Manager in the event that you happen to **forget the Master Password** previously set up for your account.

   ❍ You can press **Close** when done.

9. Create a **4-digit PIN**, so if you switch to another app and then return to Password Manager, you won't have to re-enter the master password

you set up previously. If available, you can also enable face recognition or fingerprint authentication.

The installation on your iOS / iPadOS device is now complete!

8.2.3. Shared Plan

Bitdefender Password Manager Shared Plan enables multiple users to access and utilize the same subscription. It provides a centralized approach to software access, administration, and support.

❍ The person in charge of the shared subscription plan, known as the Plan Manager, can share the service among the members.

❍ Each member gets their own unique **Bitdefender Central** account linked to their email address and access to the Bitdefender Password Manager service.

Sharing Bitdefender Password Manager with multiple users

Inviting members

To add one or multiple users to the shared subscription, the plan manager must follow these steps:

1. Log in to your Bitdefender Central account at

2. Go to the **My Subscriptions** menu located on the left side of the page.

3. Choose **Invite member** in the **Bitdefender Password Manager Shared Plan** panel.

4. Enter the email of each person you wish to share your subscription with, then click on **Send**. A maximum of 3 members can be added at once.

5. Setup instructions are emailed right away to the new members. Click on **Close** to exit the confirmation window.

> ⓘ **Note**
> Members have 24 hours to accept your invite once it's emailed to them.

- ❍ Invited members will appear with the status "Invited".
- ❍ You will see them as "Active" members after they accept the invitation. You are also notified by email of each accepted invitation.

Removing members

Bitdefender Password Manager Shared Plan access is lost for members who are removed. When the plan manager decides to remove a subscription member, the member receives an email notification. For the following 30 days, the ex-member is switched to a 30-day Bitdefender Password Manager **trial version** with full capabilities. The service will then be turned off.

The plan manager can eliminate users from the shared plan in the following way:

1. Log in to your Bitdefender Central account at
2. Go to the **My Subscriptions** menu located on the left side of the page.
3. In the **Bitdefender Password Manager Shared Plan** panel click on **Manage**, then choose **Edit members** in the menu.
4. Click the **Remove** button to take a member off the shared plan.
5. Choose **Yes**, remove member then click the **Finish editing** button for the changes to take effect.

> ⓘ **Note**
> When a member is deleted from the shared plan, their status is changed to **Pending removal** until they are completely eliminated.

Accepting an invitation

You will receive an email when someone invites you to become a subscription member for Bitdefender Password Manager Shared Plan. You have 24 hours to accept an invite once it's sent to you.

To accept the invite and gain access to the password manager features, the user must follow these steps:

1. Open the email you received titled **[Start using your Bitdefender subscription as a Member]** and click the **ACTIVATE IN CENTRAL** button.

2. The Bitdefender Central page will then open in your browser.

   ❍ If you already have a Bitdefender user account associated with the email where the invitation was sent, **sign in** to claim your shared subscription.

   ❍ If you don't have a Bitdefender user account, click on **Create one** and sign up with the same email where the invitation was sent to claim your shared subscription.

      ❍ Enter your full name

      ❍ Enter your email address

      ❍ Enter your password

      ❍ Click the **Create Account** button and you will be signed.

3. After signing in, click on **Get started** on the welcome screen that informs you that your Bitdefender Password Manager subscription is now active.

4. Follow the on-screen steps also described in Installation (page 242).

> **(i) Note**
> The plan manager's email is displayed in your Bitdefender Central account at the top of the Password Manager menu and on the subscription card, under My Subscriptions.
>
> If you need assistance with the shared plan, please get in touch with them.

8.3. Importing & Exporting your passwords

Bitdefender Password Manager is built in such a way as to efficiently facilitate communication and data transfer with external sources, platforms and software tools. This is the core reason why the very frequently encountered need of importing or exporting passwords into or out of Bitdefender Password Manager can be satisfied with ease.

8.3.1. Compatibility

Bitdefender Password Manager can seamlessly transfer data from the following list of applications:

❍ **1Password**

❍ **Bitwarden**

❍ **Bitdefender Password Manager**

❍ **ByePass**

❍ **Chrome browser**

❍ **Claro**

❍ **Dashlane**

❍ **Edge browser**

❍ **ESET Password Manager v2**

❍ **ESET Password Manager v3**

❍ **StickyPassword**

❍ **Watchguard**

❍ **Firefox browser**

❍ **Gestor de contraseñas – Claro**

❍ **Gestor de contraseñas – SIT**

❍ **Gestor de contraseñas – Telnor**

❍ **KeePass 2.x**

❍ **LastPass**

❍ **Panda Dome Passwords**

❍ **PassWatch**

❍ **Saferpass**

❍ **SFR Cybersécurité**

❍ **SIT**

❍ **F-Secure**

❍ **Telnor**

> **ⓘ Note**
> If the name of the browser or password manager tool from which you are trying to transfer data files is not mentioned in the list provided above, you can follow our online guide on how users can edit a CSV file from unsupported password managers so that you can import your information into **Bitdefender Password Manager**: https://www.bitdefender.com/consumer/support/answer/2472/

This transfer of data between Bitdefender Password Manager and other account management software can be done through the following data formats:

CSV, **JSON**, **XML**, **TXT**, **1pif** and **FSK**.

8.3.2. Importing into Password Manager

Bitdefender Password Manager allows you to easily import passwords from other password managers and browsers. If you are currently looking to switch to Bitdefender Password Manager from another password managing service, you have most likely stored a considerable amount of credentials such as usernames, passwords, and other login data required for all your accounts.

Now that you've chosen Bitdefender Password Manager, you will be looking to import that saved data into it.

Here is how to import your stored information from other apps and web browsers into Bitdefender Password Manager, **regardless of the operating system** on which you have chosen to install this product:

1. Click the Password Manager icon in your web browser (on Windows or macOS) or launch the Password Manager application (on Android or iOS). If prompted, enter your Master Password.

2. Open the Password Manager ☰ menu to expand the sidebar on the left and click the ⚙ **Settings** menu item.

3. Scroll down to the **Data** section and click on the **Import Data** option.

4. Use the drop-down menu to select the name of the password manager app or browser you want to import your accounts from. Input your Master Password in the corresponding field, then click on **Choose File**.
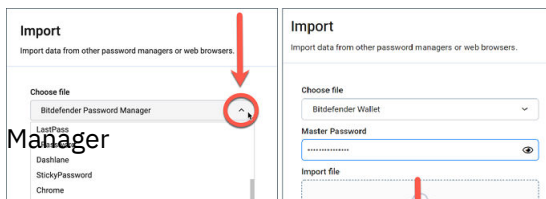
5. Browse through your folders to find the location in which you have saved the file containing your usernames and passwords, exported from your other password manager or web browser, then press **Continue**.

Once imported, your passwords will then be accessible on all devices where Bitdefender Password Manager application or browser extension is installed.

8.3.3. Exporting from Password Manager

Bitdefender Password Manager allows you to easily export your saved passwords (including account login credentials, secure notes, etc.) into a CSV (comma-separated values) file or an encrypted file if you ever wish to switch to another password manager service, so that your departure from Bitdefender Password Manager will not be a difficult process.

> ⚠ Important
>
> A CSV file is **not** encrypted and contains usernames and passwords in plain text format, meaning your private information can be read by anyone having access to your device. We therefore recommend you follow the instructions below on a trusted device.

Here is how you can export your data from Bitdefender Password Manager:

1. Click the Password Manager icon in your web browser (on Windows or macOS) or launch the Password Manager application (on Android or iOS). If prompted, enter your Master Password.

2. Open the Password Manager menu to expand the sidebar on the left and click the ⚙ **Settings** menu item.

3. Scroll down to the **Data** section and click on the **Export Data** option.

4. Now you should be prompted with the following two options:

   ❍ **CSV**

   ❍ **Password-protected files**

   Select your preferred option, then input your Master Password, and click the **Export data** button.

> **(i) Note**
> If you pick the password-protected file option, you will be asked to encrypt the data containing the accounts list with a password, so this way only you would be able to access it if needed.

5. Your web browser/app will proceed by saving a file named Bitdefender Password Manager_exported_data_current-date to your system in the default download folder. It contains all your data stored in Bitdefender Password Manager.

After exporting your data, you can upload it to the password manager of your choice.

8.4. Features & Functionalities

This chapter will take you through all features and functionalities of Bitdefender Password Manager, explaining their usefulness and how to operate them most efficiently.

8.4.1. Password Handling

Password Generator

The golden rule in regards to online security is to always use unique random passphrases for every service that requires account creation. Password reuse across multiple platforms is the number one reason behind identity theft and losses associated with hostile account takeover.

This feature helps users with generating secure, complex, and unique passwords for every new account they create anywhere online. This eliminates the need for users to come up with strong passwords on their own or being careful not to reuse the same password for multiple accounts.

The ⊚ **Password Generator** can be accessed through the tab on the top of the Password Manager interface.

The generator can be set to return passwords **between 4 and 32 characters**.

You can also specify the types of characters that should or should not be present in the randomly generated password by checking or unchecking the corresponding tick boxes. **(Lowercase, Uppercase, Numbers, Special)**

By pressing the ↻ button to the right of the displayed password, the generator will change the suggested password.

To use the displayed password, press **Use password**, action which will save the string of characters to your clipboard.

> **i** Note
> Your previously generated passwords will be temporarily stored in Password history, which can be accessed through the **Password history** button.

Password Capturing

With this feature within Password Manager, you will be prompted to store all of your new passwords immediately after creating them. Password Manager will prompt users to store their newly created passwords, so that they may be added to the ultra-safe environment provided by Bitdefender right away.

Intelligent Autofill

Bitdefender Password Manager can be set up in such a way that it can autofill your login credentials and most importantly passwords. Proprietary algorithms can detect and pre-fill credentials on previously visited websites, saving the users' time every time they log in to a service.

1. On Windows or macOS, click on the 🛡 **Password Manager** icon in your web browser.
   On Android or iOS, launch the 🛡 **Password Manager** application.
   If prompted, enter your Master Password.

2. Open the Password Manager menu ☰ to expand the sidebar on the left and click the ⚙ **Settings** menu item.

3. Click on **Device Settings**.

4. Here you will notice a button displaying either **Disable Auto-Fill** or **Enable Auto-Fill**. This setting controls the operating state of the intelligent autofill feature.

Security Report

The Security Report is a tool that will generate reports based on a number of features meant to bolster your digital security. It will let you know if

a password requires your immediate attention by determining its level of security. It will detect password duplicates and prompt you to change them accordingly, avoiding the dangers of recycling the same passwords for multiple accounts.

The report will concentrate on providing you with information on your overall password hygiene: this refers to duplicate passwords, weak or otherwise leaked passwords or email addresses.

This is done by comparing the list of encrypted hashes from Troy's webpage locally on your device to check if it contains the corresponding hashes of your passwords. If a match is to be found, you will be notified so as to encourage you to consequently change your passwords and other login credentials.

To access the **Security Report**, enter the Password Manager interface and select its corresponding ⬚ button in the top bar.

Sync Across Other Platforms

Saving your passwords once into Bitdefender Password Manager will enable you to store and securely access them on all your Windows, Mac, Android or iOS devices from Chrome, Safari, Firefox and Edge or inside mobile apps.

> **ⓘ** **Note**
> Bitdefender is also equipped with an **offline mode** to access your passwords, in the event that you happen to not have access to the internet. This makes your passwords accessible at all times and from anywhere.

Deleting an entry

To delete saved passwords first press the ✎ edit icon next to the entry you want to remove, located in the ⛊ **Accounts** tab. Scroll down then choose **Delete**. When asked if you are sure you want to remove the account select **Remove**.

8.4.2. Account Handling

Authentication

The Authentication into Bitdefender Password Manager is done through the **PIN** set up in the installation process of the product. (Note that the

Auto-Lock feature will lock the password manager or logout after a period of inactivity at browser level or closing the mobile app)

Additionally, it can also be done through the use of biometrics, if available, such as **Fingerprint** or **Face unlock**.

To **enable or disable** biometry-based authentication:

1. On Windows or macOS, click on the 🛡 **Password Manager** icon in your web browser.
   On Android or iOS, launch the 🛡 **Password Manager** application.
   If prompted, enter your Master Password.

2. Open the Password Manager menu ≡ to expand the sidebar on the left and click the ⚙ **Settings** menu item.

3. Click on **Device Settings**.

4. Here you will notice a button displaying either **Disable biometry** or **Enable biometry**. This setting controls the operating state of the biometry-based authentication feature.

Master Password Reset

⚠ Important
The **Change Master Password** feature is not available on mobile devices. The only way you can change or recover your master password is via the Bitdefender Password Manager browser extension on a Windows PC or a macOS device.

Here's how to change your Master Password as a precautionary measure and create a new one in Bitdefender Password Manager:

1. Once you have the browser extension installed, click the 🛡 **Password Manager** icon in your web browser toolbar.

2. Enter your current master password to unlock the vault.

> **⚠ Important**
>
> If you do not remember the current master password, click the **I've forgotten my password** option on the same screen. Enter the **24-digit Recovery Key** provided during the initial Bitdefender Password Manager setup, then type a new master password. **If you forget or misplace** both the Master Password and the **Recovery Key**, as a last resort, **contact a Bitdefender representative to help reset your account**. Resetting your account will erase all your data and passwords saved in Bitdefender Password Manager.

3. Open the Password Manager menu ☰ to expand the sidebar on the left and click the ⚙ **Settings** menu item.

4. Click on the **My account** button in the **Account** section.

5. A window with information about your Password Manager subscription will be displayed.
   Click on the **Change Master Password** button.

6. You'll be redirected to a new window where you can choose a new master password. Enter your current master password, then type a new master password. The new master password must contain a minimum of 8 characters, at least one lowercase letter, one uppercase letter, and one number.

7. Press the **Change** button when you're done.

8. Wait a few moments until Bitdefender resets the old master password. Do not exit your web browser!

9. Next, you are provided with a new **24-digit recovery key**. Make a note of the recovery key in a safe place and **don't lose it**. This key is the only way to access your passwords saved in Password Manager in case you forget the master password.
   Press **Close** when you're done.

10 You will be logged out of Bitdefender Password Manager.
· To unlock the vault, use the new master password you just set.

8.4.3. Other functionalities

Identities management

This feature allows users to store multiple identities and lets Password Manager automatically fill in details in web forms before making a purchase in a quick, easy and secure manner.

Like everything else in Password Manager, all sensitive data contained within these stored identities is encrypted and available only to the user's device.

To add an identity to Password Manager:

1. On Windows or macOS, click on the 🛡 **Password Manager** icon in your web browser.
   On Android or iOS, launch the 🛡 **Password Manager** application.
   If prompted, enter your Master Password.

2. Open the Password Manager menu ☰ to expand the sidebar on the left and click the 🖼 **Identities** menu item.

3. Press on the **Add Identity** button at the bottom.

4. Complete the details you want stored then press **Save**.

Credit Card management

This feature allows you to save and fill credit card details for easier, faster and more secure shopping.

To add a credit card to Password Manager:

1. On Windows or macOS, click on the 🛡 **Password Manager** icon in your web browser.
   On Android or iOS, launch the 🛡 **Password Manager** application.
   If prompted, enter your Master Password.

2. Open the Password Manager menu ☰ to expand the sidebar on the left and click the 🖼 **Credit cards** menu item.

3. Press on the **Add Identity** button at the bottom.

4. Complete the details you want stored then press **Save**.

Secure Me

The Secure Me feature allows you to remotely log out or delete browsing history of your computer, tablet or mobile device. If you're sharing a device with other people, we strongly recommend you turn this feature on.

To locate and enable this feature:

1. On Windows or macOS, click on the **Password Manager** icon in your web browser.
On Android or iOS, launch the **Password Manager** application.
If prompted, enter your Master Password.

2. Open the Password Manager menu to expand the sidebar on the left and click the **Secure Me** menu item.

3. Press on the **Secure all sessions** button.
If you are looking to secure only a particular device, look for it in the list of devices on which Password Manager is installed or enabled on a specific browser.

Notes

Secure Notes is a feature that acts just like a secret notebook where you can store sensitive data, sort it and use color coding to better visualize it. Not only does it keep information tidy, but you also keep it safe and secure.

To locate and enable this feature:

1. On Windows or macOS, click on the **Password Manager** icon in your web browser.
On Android or iOS, launch the **Password Manager** application.
If prompted, enter your Master Password.

2. Open the Password Manager menu to expand the sidebar on the left and click the **Notes** menu item.

3. Press on the **Add note** button.
Once you have written down the information you want to safekeep, press **Save**.

8.5. Frequently Asked Questions

Some common questions about Bitdefender Password Manager tend to recur. We have the answers! Here you can learn more about your Bitdefender account, importing passwords, data security protocols, and other topics important to our customers.

General questions about Bitdefender Password Manager

How do I stop the Password Manager pop-up in my Bitdefender security solution?

The Password Manager notification displayed by Bitdefender Total Security, Internet Security, and Antivirus Plus in August 2022 can be dismissed by clicking the "x" button. The "Manage your passwords with Bitdefender Password Manager" window will randomly reappear a couple of times before disappearing forever. You can opt out of this promotional message by toggling **Recommendation notifications** to the off position in Bitdefender Settings.

What happens when Bitdefender Password Manager expires?

Once your Password Manager subscription expires and is no longer active, you will have a maximum of 90 days to export your passwords. Your passwords will be backed up for another 30 days. During those 90 days, you will only be able to export your data. You cannot continue to use Password Manager. The auto-fill feature will stop working, as well as the ability to generate passwords.

At the end of the 90-day grace period, you have 30 extra days to contact Bitdefender support and request to restore your passwords back to the live database. You will then be able to export your passwords from Bitdefender Password Manager.

Your data will be kept in the live database only until the end of the day it was restored on demand. At midnight the database is erased – and if you have not yet exceeded the 30-day extra period, passwords can be restored again from backup. Raw database data from the backup can be provided upon request to the user, but the database is encrypted and the information cannot be accessed.

What is a Master Password, and why do I have to remember it?

The Master Password is the key that unlocks the door to all the passwords stored in your Bitdefender Password Manager account. The master

password must be at least 8 characters long. So create a strong master password, memorize it, and never share it with anyone. To create a strong master password, we recommend you use a combination of uppercase and lowercase letters, numbers, and special characters (like #, $, or @).

How can I stop Bitdefender from asking for my Master Password every time I open the browser?

If you lock your device without closing your browser, Password Manager doesn't lock and you can access your data when you return. As a security measure, every time you open the browser you have to sign in with your Bitdefender Central account and then input your Master password.

❍ To stop the Central sign-in prompt, go into Settings and tick "Disable login tab on startup".

❍ To stop the master password prompt, check the "Remember me" box on the Unlock your vault screen.

Why don't you store my Master Password, and what happens if I forget it?

The reason why we don't store your Master Password on our servers is so that only you can access your account. It's the most secure way. If Bitdefender Password Manager doesn't recognize your master password, make sure you type it correctly and the Caps Lock key is not active on the keyboard.

If you forget the master password, you can always use the Recovery Key to unlock Password Manager. During the sign-up process, Bitdefender Password Manager provides a **recovery key** that can be used to regain access to the account without losing your data.

If you forget or misplace both the Master Password and the Recovery Key, as a last resort, contact a Bitdefender representative to reset your account.

> ⚠ Important
> Resetting your account will erase all your data and passwords saved in Bitdefender Password Manager.

Can multiple users share one Bitdefender Password Manager subscription?

For now, the ability to have multiple users on the same Password Manager subscription is not available but we are working on enabling this feature in the near future.

What is Offline mode and how does it work?

Offline mode is automatically activated when the Internet connection drops while using Bitdefender Password Manager. If you are already signed in and have entered your master password, Offline mode lets you access your passwords when an Internet connection is out of reach.

How do I uninstall Bitdefender Password Manager?

To uninstall Bitdefender Password Manager:

❍ On Windows and macOS:
  Remove the Password Manager extension from your web browser. Right-click on the Bitdefender icon and select "Remove".

❍ On Android:
  Tap and hold the Password Manager app, then drag it to the top of the screen where it says "Uninstall".

❍ On iOS & iPadOS:
  Tap and hold the Password Manager app until all apps on your screen begin wiggling, then tap the X to the top left of the Bitdefender icon.

Privacy & Security questions about Bitdefender Password Manager

Could Bitdefender employees see my passwords?

Absolutely not. Your privacy is our top priority. This is the main reason why we do not store your master password on our data servers: so that no one has access to your account, not even company employees. Every password and account are highly encrypted with the strongest data security algorithm, and the code we see simply looks like a random string of numbers and letters jumbled together.

What would happen if Password Manager servers were hacked?

Each password is encrypted locally on your device before it gets anywhere near our servers, so if hackers were to break into our system, they would only get pages of random letters and numbers without your key to decrypt them. This means that you and your account details are always safe with us.

9. DIGITAL IDENTITY PROTECTION

9.1. What is Bitdefender Digital Identity Protection

Online privacy and security are some of the main focuses for internet users nowadays. And there are some very good reasons for that. With major data breaches happening more often than not, it is imperative to make sure that your personally identifiable information (PII) is safe and secure.

But what can be classified as personally identifiable information? Traditionally, sensitive information such as the full name, social security number, driver's license, mailing address or credit card information were considered PII. Eventually, less-sensitive info, such as zip codes, IP addresses, or login IDs were also included. Over time, your digital footprint, meaning the data you leave behind as a result of your browsing the internet, might come to include some of these.

Bitdefender Digital Identity Protection represents the private way to online freedom, allowing you to regain control of your digital life. And it requires only your name, most used email address and your phone number. Based on these, it searches on both the Surface Web and the Dark Web for personal information that was exposed publicly.

Bitdefender Digital Identity Protection offers the following:

❍ **Monitoring and detection services:** it monitors more than 100 personally identifiable information such as SSN, credit cards or home address, and displays all data found about your online footprint.

> ℹ️ Note
> Bitdefender does not store or process personally identifiable information. Only references to potential data breaches are kept, without including sensitive data.

❍ **Real-time alerts:** You receive notifications about data breaches and exposed data in Dark Web, personal information in Surface Web and potential impersonators you on social media.

❍ **Solutions:** Our service suggests clear actions required to solve issues and provide reminders if an issue is not solved entirely. It can also

provide instructions on how to remove the personalized ads, export your data, or turn off the tracking.

9.2. Getting Started

9.2.1. Activate Digital Identity Protection

Activate the Bitdefender Digital Identity Protection subscription after your order is placed and paid.

1. Open the confirmation email received shortly after completing your order and click on **GET STARTED**.

2. You will be redirected to https://central.bitdefender.com.
   Sign in with your Bitdefender Central account. If you don't have an account, choose to create one.

3. After signing in, the subscription will automatically be attached to your Central account and will trigger the onboarding process.

Alternatively:

❍ access the **My Subscriptions** panel from Central, located on the left side of the window, and click **+ Activate with code**.

❍ type in the 10 digit-key found in your confirmation email and press **ACTIVATE**.

❍ if prompted, select how you would like to use the code, then click on **ACTIVATE**.

9.2.2. Configure Digital Identity Protection

1. Go to https://central.bitdefender.com/ and sign in to your account.
   If you don't already have an account, click on **CREATE ACCOUNT**, then type your full name, an email address and a password.

2. Select the Digital Identity Protection panel.
   A welcoming screen is displayed.

3. Click **BEGIN**.

4. You will now be informed on what information you need to provide. Your data will always be encrypted and secured.
   Click **NEXT**.

5. Type your first name, middle name (if any) and last name in their corresponding boxes, then click **NEXT**.

6. Type your email address, then click **NEXT**.
    Make sure it is a valid email address you can access.

7. A security code is sent to the address you provided.
    Open your email, copy the code and paste it in its corresponding field.
    After that, click **CHECK**.

8. Select your country and enter your phone number, then click **NEXT**.

9. You should receive a security code shortly after that.
    Enter the code, then select **CHECK**.

10 After the initial check is performed, click **FINISH**.
.

> **(i) Note**
> You will be informed if any breaches, personally identifiable information or potential impersonation attempts are discovered during this first check.

Bitdefender Digital Identity Protection is now configured.

9.2.3. Review your Digital Footprint, Data Breaches and possible Impersonations

After you complete the configuration, Bitdefender Digital Identity Protection performs an online check to discover potential impersonations, data breaches and personally identifiable information on the Open Web. We recommend reviewing every piece of info included in the **DIGITAL FOOTPRINT**, **DATA BREACHES** and **IMPERSONATION CHECK** tabs.

❍ Reviewing your Digital Footprint (page 267)

❍ Reviewing Data Breaches (page 267)

❍ Reviewing possible Impersonations (page 268)

9.2.4. Improve your check-up

We use the data you provide to monitor the Surface Web and Dark Web to detect any activity that might affect your privacy or your personal brand reputation.

If you would like to add another email address or another phone number, click ➕, then click on **ADD EMAIL ADDRESS** or **ADD PHONE NUMBER** and follow the instructions.

9.3. Dashboard

The Dashboard aggregates information included in the **DIGITAL FOOTPRINT**, **DATA BREACHES** and **IMPERSONATION CHECK** sections.

It includes the following:

❍ Your exposed data and their web sources

❍ The average amount of exposed data for the entire community

❍ Your Digital Footprint evolution

❍ Privacy-related content

❍ Data Breaches

❍ The average number of data breaches inside the community

9.3.1. Digital Identity Monitor

Using only accurate information Bitdefender's system looks for new personal data exposed on the Open Web and Dark Web and scans all the major Social media platforms for any signs of an impersonation attempt.

Click on **CHECK NOW** to perform an online scan.
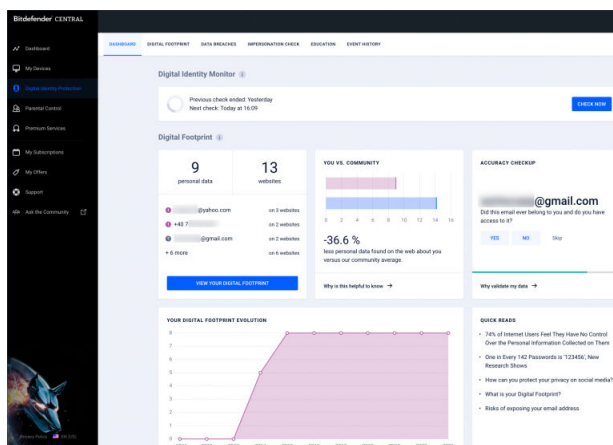
9.4. Digital Footprint

Your personally identifiable information and their sources appear here. It is up to you to evaluate if having the information public on the web is a threat.

Our AI-driven monitor relies heavily on correct data to detect new threats, so please tell us if the information is accurate or inaccurate.

Once you confirm a piece of information is yours, we add it to our monitoring system and improve the chances of discovering other ones in the future.

9.4.1. Reviewing your Digital Footprint

To review your digital footprint:

1. Go to the **DIGITAL FOOTPRINT** tab.

2. Information that has not been verified yet will appear with the text **Verify** on the right side. Click **Verify**, then select Yes or No, depending on the case.

> **i** Note
> Every piece of information confirmed is added to our monitoring algorithm, improving the results displayed by our services. Information that is dismissed will no longer be displayed. However, it will still remain available on the web.

9.5. Data Breaches

Breaches occur when hackers manage to bypass a company's security measures and obtain your personal information, to sell it on the dark web. Typically, cybercriminals target login data, personally identifiable information (PII), medical records, and banking-related details.

Any organization or service can fall victim to a data breach, but those with a large consumer base make more attractive targets. Breaches commonly include names, email addresses, usernames, passwords, postal addresses, phone numbers, social security numbers (SSN) and credit card data (number, expiration date, CVV).

9.5.1. Reviewing Data Breaches

To review your data breaches:

1. Go to the **DATA BREACHES** tab.

2. Under some entries, you will find a list of actions required for securing your account. After performing an action, click the box next to it in order to confirm.

   If you're not sure about how to perform a task, you can always click on the link included in the task description and you'll be redirected to a page where you'll find all the necessary steps.

   Not all breaches can be dealt with in this manner. Some of them, such as **Collection #1**, won't include steps. Instead, you will be redirected to articles available online where you can find more help.

   > **i** Note
   > Bitdefender does not store or process personally identifiable information. Only references to potential data breaches are kept, without including sensitive data.

9.6. Impersonation Check

Criminals known as "pretexters" use the art of impersonation in many ways, playing the role of a trusted individual to deceive their victims and gain access to sensitive information. The practice of "pretexting" is defined as presenting oneself as someone else to manipulate a recipient into providing sensitive data such as passwords, credit card numbers, or other confidential information.

Bitdefender Digital Identity Protection monitors 25 Social Media platforms and notifies you instantly if it finds a profile that could be an impersonation attempt.

9.6.1. Reviewing possible Impersonations

The **IMPERSONATION CHECK** tab is where all possible attempts will be displayed. For each detection, you can choose one of three possibilities:

❍ It is an impersonation attempt

❍ It is your own profile

❍ It is a different profile

Depending on the choice, Bitdefender Digital Identity Protection will recommend specific steps in order to deal with the issue. Every time you complete a step, you can mark it as **Done**.

9.7. Education

The Education tab serves as a knowledge base where the user can find more information on how to protect their digital identity.

Articles listed here can be sorted into several categories:

❍ Breaches

❍ Exposures

❍ Impersonation Check

To access the full version of an article, click on its corresponding **Read more** link.

9.8. Event History

The Event History section is the means by which we communicate constantly with our users. It represents a chronologically ordered list of events regarding the protection of your Digital Identity.

Besides newly detected threats (if any), you can return to this page for valuable advice on how to properly conduct yourself online, to increase the chances of not dealing with privacy issues.

In the Event History section, you can find the following information:

❍ Actions performed

❍ Service updates

❍ Data Breaches

10. GETTING HELP

10.1. 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.

10.2. 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.

10.2.1. 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/.

10.2.2. 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/

10.2.3. 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/.

10.3. 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/

10.3.1. 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.