AntiLeaks VPN Router

Quick Guide

Important Information (Privacy)

AntiLeaks VPN Router is an Internet privacy device. It encrypts your traffic and prevents your location from being discovered by the IP address, but it cannot protect you if you identify yourself.

When a user logs in to Facebook, for example, he receives a "cookie" through which he starts to be tracked. When that user visits a website that contains some Facebook code on its pages, Facebook immediately identifies that person. Note that Facebook is just an example. He's not the only one who does that.

The "cookies" received by your web browser are one of the ways in which you can be identified, even on sites where you have never been. Make sure to delete all cookies from your browser BEFORE accessing any website where you do not want to be identified. You can also use the web browser in privacy mode. In the case of Google Chrome, the shortcut to open a navigation window in privacy mode is SHIFT + CTRL + N.

Whoever inserts codes provided by third parties on the web pages of their website, with external calls, puts the privacy of users at risk. Complain to the person in charge of the site and run away from sites that do this.

Examples of sites that pose risks to your privacy and data security:

TAny and all websites that incorporate advertisements generated by Google and other external sources

Any and all websites that incorporate content generated by Facebook or other social networks

Any and all sites that incorporate a visit counter provided by third parties, such as Google Analytics

Any and all websites that incorporate code / element obtained dynamically from third party servers. It can be a javascript code, often called "javascript framework" or any other element (image, video, file) of external origin. This scenario represents a security risk and systematically exposes visitor data to the server from which that code / element is being "pulled".

Before turning on your AntiLeaks (Prerequisites)

<u>Internet access with IPv4 addressing</u>

AntiLeaks needs IPv4 to work. If your Internet access has only IPv6, complain to your ISP and ask them to activate IPv4. Your (pre-existing) router must receive a valid IPv4 address on the WAN port. IPv4 is an Internet addressing standard used by the vast majority of providers worldwide.

You do not need to understand this to use AntiLeaks. We just want you to know that if your AntiLeaks is unable to connect this may be one of the causes. In case of difficulties with your connection, contact our technical support and we will be able to assist you.

<u>VPN Access Card</u>

To connect to our VPN servers distributed around the world you need an access card. Your AntiLeaks comes with a free access card, which allows you to use our VPN service for 30 days.

Additional cards with different VPN service plans (1, 3, 6 and 12 months in duration) can be purchased at https://antileaks.com. Each card contains an activation code which you use to redeem and activate the respective plan.

VPN Access Card redemption

Once you have your access card number, access the website https://antileaks.com and look for the option "Redeem Card".

Once on the redemption page, enter the 32-character-long code that appears on the card into the gap. It consists of numbers and capital letters.

On the next page, you will see information about the access card and the current status, that is, whether it has already been activated or not. Activate your VPN access plan by clicking on "ACTIVATE NOW"

Your VPN service access credentials (login / password) will be generated.

Make a note of the "VPN Username" (including the "userid0s" part) and "VPN Password". You will need to enter these two information inside your AntiLeaks device. (Note: If the "VPN Password" is hidden, click on the "SHOW" button to display it)

IMPORTANT NOTE (DATA SECURITY): Never give your access card number to other people or your VPN access credentials. With the card number, anyone can access the redemption section above and see their credentials. Make sure to keep your data in a safe place.

Physical installation of AntiLeaks

Choosing the ideal location

AntiLeaks needs to be connected to your network via the cable that comes with it. AntiLeaks is designed to stay on your desk, next to your computer, but if you don't have a network cable connection point next to your computer, place it next to your Internet router or anywhere else on your network with Internet access. Also make sure you have a power outlet available to turn on AntiLeaks.

NOTE: Please note that the AntiLeaks Wi-Fi signal has a limited range, complying with the permitted power / frequencies of radio waves. If AntiLeaks is placed too far away or is behind walls, the Wi-Fi signal range will be affected.

Connecting the network cable

AntiLeaks can be connected to any available LAN port on your network, with Internet access. This port can be the output of your Internet router, a free LAN port on a switch / hub or any other point on your local network.

AntiLeaks has 2 RJ45 ports. **Connect the network cable to the right port of AntiLeaks.**

The RJ45 port positioned on the left has another function. Read the **AntiLeaks Operation Manual** to understand its purpose and learn how to use it.

Connecting the power supply

Your AntiLeaks comes with a 5V USB power supply and its USB cable with an on / off switch.

Plug one of the terminated cables into the source and the other into the Micro USB port on AntiLeaks.

Turning on for the first time

Once the network and power supply cables are connected, insert the power supply into the outlet and activate the switch located on the power supply cable.

In a moment, AntiLeaks will light up, start talking and the OLED display will show some information.

As soon as he finishes loading the system, he will tell you that he needs the VPN access credentials. To do this, follow the steps in the next section of this manual, **Initial Settings**.

IMPORTANT NOTE (APPLIANCE CARE): AntiLeaks, although small, is a computer and works in a similar way. When turning it on you need to wait until the operating system loads and you should also NEVER turn it off directly at the switch. You must ALWAYS give the shutdown command before turning off / cutting off its power. Turning off AntiLeaks without shutting down can corrupt data and / or damage your firmware, making AntiLeaks inoperable. Refer to the **AntiLeaks Operation Manual**.

Initial Settings

If everything has worked so far, your AntiLeaks must be on and lit and a voice must be asking for VPN credentials, which you must enter before you can start using AntiLeaks.

Your VPN access credentials ("VPN Username" and "VPN Password") need to be entered into AntiLeaks whenever you redeem a VPN access card. Without these credentials AntiLeaks will not connect to the VPN service. It is also unable to connect if you enter invalid or expired credentials.

Connect to AntiLeaks via WiFi

Connect any device (tablet, computer, cell phone) via WiFi to AntiLeaks. The name of the WiFi network is **AntiLeaks** and the default password is **antileaks** (lower case)

When you connect you will not be able to access the Internet yet, but you will be able to access the AntiLeaks configuration interface normally.

If your device (tablet, computer, cell phone) inform that AntiLeaks WiFi does not have Internet access and ask if you want to connect anyway, confirm.

Access the AntiLeaks Management Interface

Once you have connected your device to AntiLeaks open a web browser and access the following address: **http://192.168.42.1**

Then, in the username field type **admin**, in the password field type **antileaks** and click the **Login** button.

Inserting the VPN access credentials ("VPN Username" and "VPN Password")

Once inside the AntiLeaks configuration interface, click on **Control Panel**, then **VPN Management** and finally on **VPN Settings**.

Enter your "**VPN Username**" and "**VPN Password**" in the corresponding fields and click the **Save** button. (**WARNING**: Do not change any other settings without reading the AntiLeaks Operation Manual.)

If you have connected the cables and entered the VPN access credentials correctly, AntiLeaks will automatically connect and release Internet access to the device (s) connected to it. Ready! You can now use the Internet through AntiLeaks.

NOTE: Note that the first time it may take some time for AntiLeaks to find a way out, especially if you are in a country where Internet content is censored. If after 30 minutes, your AntiLeaks is unable to connect, review all steps for installing cables and initial AntiLeaks configuration. Also check that the VPN access credentials have been entered correctly.

Troubleshooting

AntiLeaks turns on, but nothing appears on the display

The firmware, which is AntiLeaks' internal software, may have been damaged. This can happen due to electricity failures or when AntiLeaks is suddenly turned off, without the shutdown command being given. To solve this problem you will have to download the firmware from our website and rewrite it on the AntiLeaks microSD memory card. Go to https://antileaks.com and visit the **Support** section, **Firmware Update**. There you will find a detailed explanation of the procedure.

AntiLeaks keeps repeating "Router is DOWN - Please verify"

This indicates that AntiLeaks is unable to connect to your network. Make sure that the cable that gives access to your network or Intenet router, is connected to the right port of your AntiLeaks. The left door has another purpose and is not used by AntiLeaks to access the Internet. If the problem persists, try replacing the network cable. Additionally, make sure that your internet router is turned on and operating normally. Once everything is connected, AntiLeaks will stop giving this warning and will try to connect.