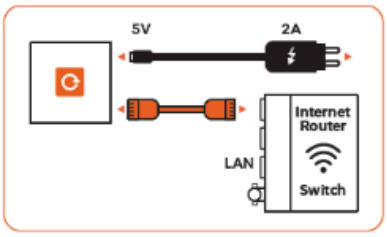
Quick Start Guide

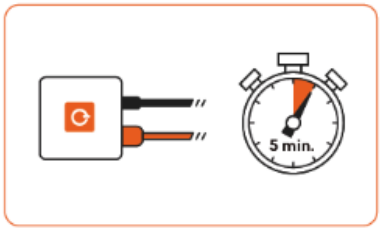
1. Plug in

- Start by connecting your eBlocker with the orange LAN cable to your router or switch **first**. Then connect the enclosed power supply to power up your eBlocker.



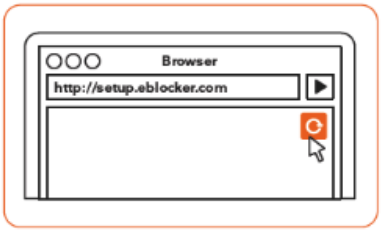
2. Auto-Configuration

- Please wait for 5 minutes to let eBlocker configure itself automatically. Then start a web browser and go to http://setup.eblocker.com



3. Play

- The eBlocker Icon appears at the top right corner of the browser window. Click on the Icon to open the Controlbar, in which you can read the most important information about the page you are currently visiting. You are able to customize the settings here.

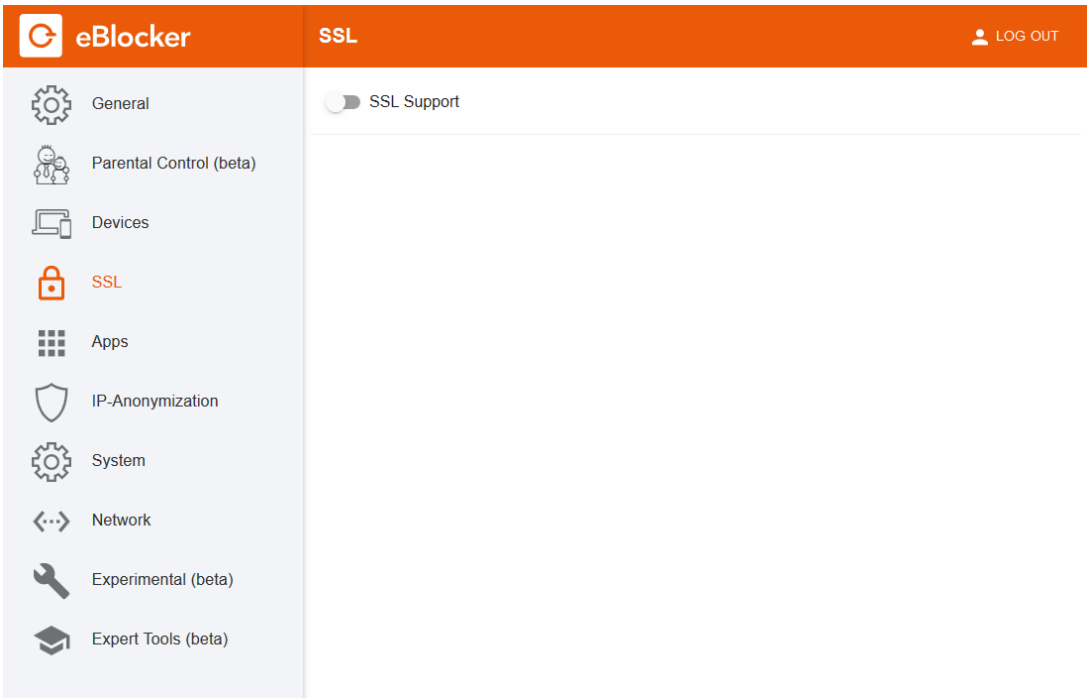


4. Activating SSL (optional for HTTPS protection)

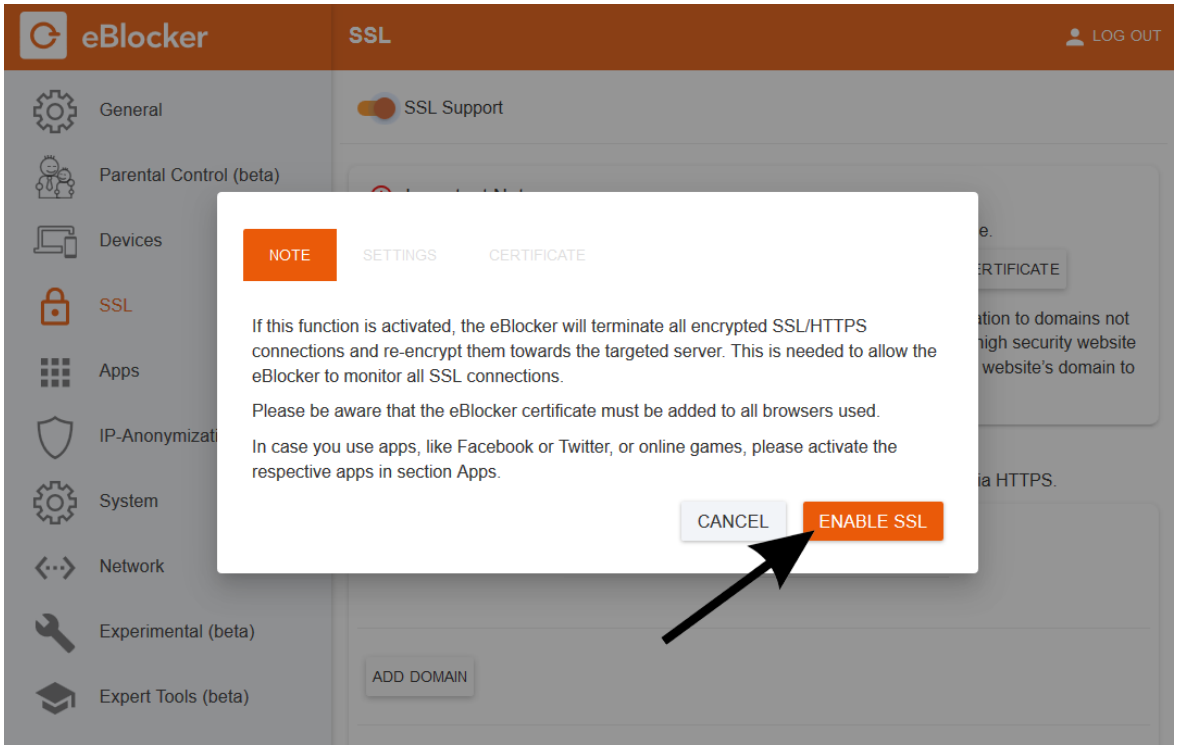
In order to protect encrypted communications (i.e. SSL/HTTPS-connections) too, SSL needs to be enabled on the eBlocker. As soon as SSL is enabled, eBlocker terminates encrypted connections to analyze the data stream and encrypts the data again before transmission to the browser. **For this encryption it is necessary to add the individual security certificate of your eBlocker in all your browsers and devices once**.

Enabling SSL and adding the certificate is easy:

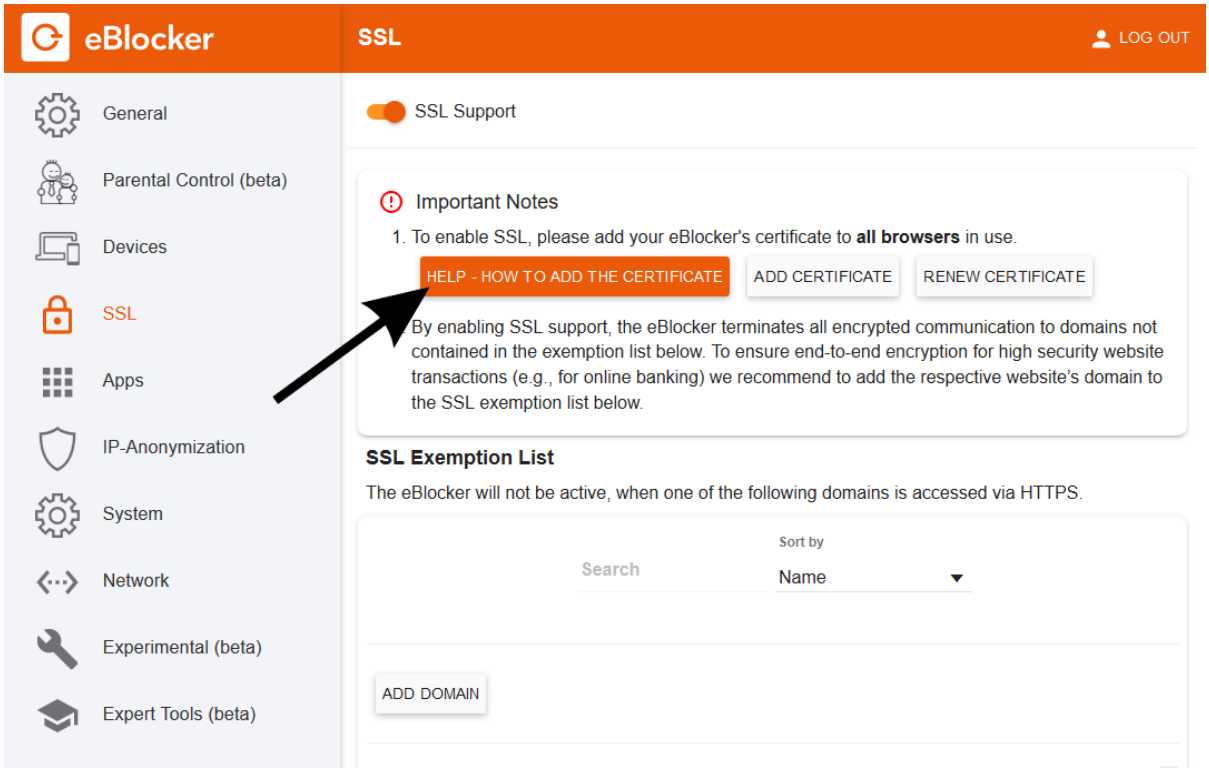
- Click on the eBlocker icon at the top right of your browser and go to “Settings”.
- Click on the menu item “SSL”. Activate SSL by switching the button to the right.



- A short note appears that the eBlocker will terminate all encrypted SSL/HTTPS connections and re-encrypt them towards the targeted server to monitor all SSL connections.
- Please read and confirm the notice and click on “Enable SSL”.



- Click on ”Help – how to add the certificate” below “Important notes” to get detailed information about adding the certificate to your particular browser.

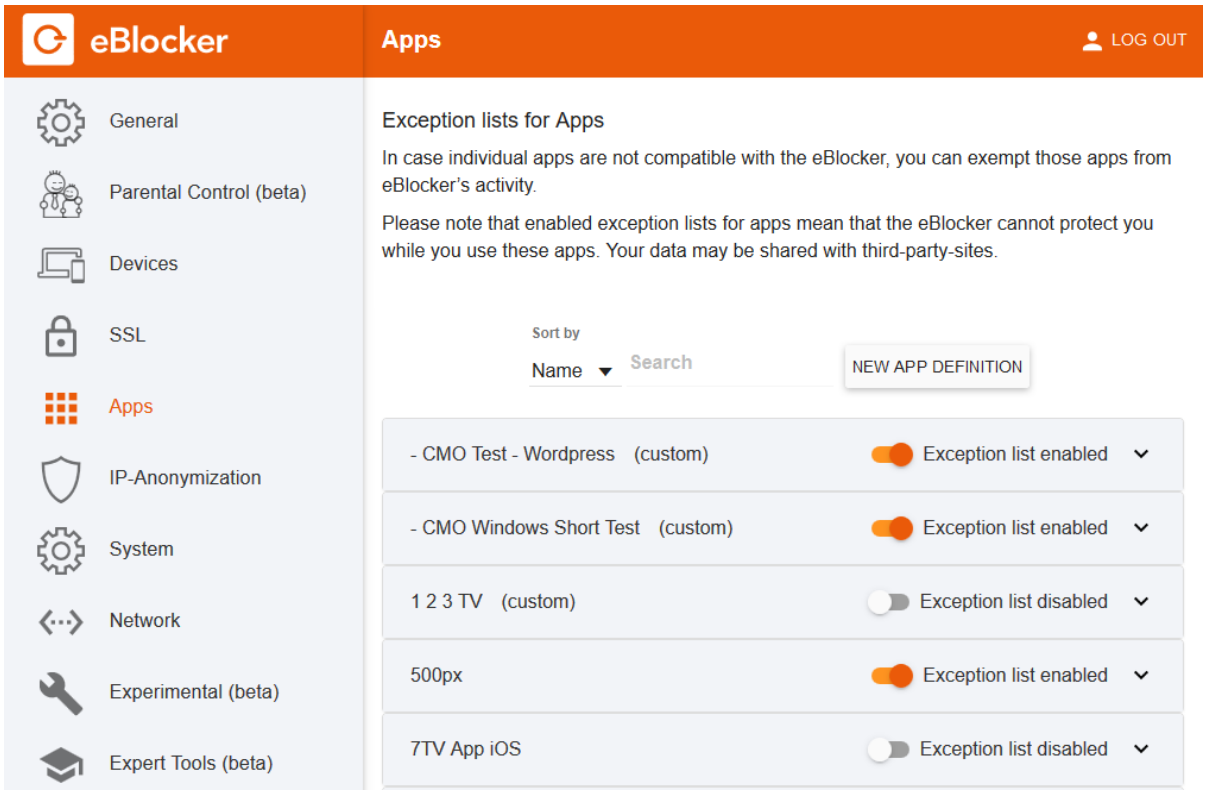


- Please note that every certificate needs to be added in **every single browser you use** individually. *Read the appendix below how to add the certificate for your particular OS. In addition section 6.2 in the eBlocker manual covers most common OS and browsers in detail.*

5. Defining App exceptions

Browsing the internet with a regular Browser usually works just fine. However, if you are using Apps to access certain web services (i.e. Facebook App, Twitter App, etc.) some Apps might use intrinsic tracking and might not work properly if eBlocker is blocking the trackers. In this case you can easily define exceptions for these Apps, so that eBlocker is not interfering with the App's trackers. The App will work as usual – but you will get tracked again.

- Click on the eBlocker icon at the top right of your browser and go to "Settings".
- Click on the menu „Apps".



- A list of predefined exceptions is displayed. To except eBlocker protection for an App, activate the corresponding slider.
- If a particular app is missing in the list, please let us know. Tech savvy users can add individual exemptions by following the steps in the user manual chapter 8.5. The manual can be found at www.eblocker.com/help

6. In case of issues

Individual setup
In case you are experiencing connection issues or the speed decreases, you can setup the eBlocker individually with just a few clicks.

- Find out how to deactivate the DHCP server of your router. For details, refer to your router manual.
- Click on the "eBlocker Settings > Network" in the Network wizard.
- Read the "Preparation" and "Procedure".
- Make a note of the displayed "Settings".
- Disable the DHCP server of your router
  Confirm all three steps and click on “Perform and Reboot”.

7. Appendix

Adding the eBlocker certificate in Windows

- In Microsoft Edge or Microsoft Internet Explorer open the eBlocker Settings and select SSL in the menu.
- Click the button "Add Certificate".
- After the dialog appears, go to save and then click on open.
- Click on Install Certificate.
- The Certificate Import Wizard opens. Click on Next. Go to safe all certificates into the following storage and click on browse afterwards.
- Choose the second register Trusted Root Certification Authorities and confirm this process with OK.
- Click on Next in the Certificate Import Wizard and confirm the process with Finish.
- Confirm the following safety warning with Yes.
- Done.

- **Adding the eBlocker certificate in MacOS**
  In Safari open the eBlocker Settings and select SSL in the menu..
- Click on the button "Add certificate".
- Go to programs/applicationprograms and open the keychain Access application.
- Choose keychain system and the category certificate.
- Go to the menu and choose storage / import objects… .
- Choose the downloaded eBlocker certificate for the file dialog and click on open.
- You will eventually be asked to type the administration password.
- Double-click on the imported eBlocker certificate.
- Choose „always trust“ in the drop-down menu Secure Sockets Layer (SSL).
- Close the window. Type in the administrator password, if you are asked.
- Done.