eBlocker®

Switch on Privacy.

User Manual

Attention: This document is out-dated. Use for reference only.
The online version is up-to-date: https://eBlocker.org/docs

eBlocker GmbH

All rights reserved. Errors and omissions reserved.
eBlocker GmbH | Kaiser-Wilhelm-Str. 47 | 20355 Hamburg | Germany

eBlocker
Switch on Privacy.

Index

Introduction.....5

1.1 The eBlocker Products.....6

1.2 The eBlocker Versions.....6

1.2.1 eBlocker Base.....6

1.2.2 eBlocker Pro.....7

1.2.3 eBlocker Family.....8

2 Commissioning.....9

3 Activation.....10

4 Use eBlocker optimally.....11

4.1 Summary.....11

4.2 Deleting cookies, cache and browsing history.....11

4.3 Activate support for HTTPS/SSL encrypted connections.....11

4.4 Activate exceptions for apps.....11

4.5 Final recommendation.....11

5 If something may not work.....13

5.1 Connection- and network problems.....13

5.2 A website is not displayed.....13

5.3 The eBlocker icon does not displayed on all devices.....15

5.4 The eBlocker icon is not showing on any device.....15

5.5 Removing common problems.....16

5.6 Some apps don’t work.....17

5.7 The eBlocker completely stopped operating.....18

5.8 More help: Our forum and support.....18

6 Tips and Tricks.....19

6.1 The individual setup – eBlocker overtaking the DHCP server.....19

6.2 Adding the eBlocker certificate.....19

6.2.1 macOS.....20

6.2.2 Windows.....23

6.2.3 Android.....29

6.2.4 iOS.....30

7 Definition of eBlocker functions.....33

7.1 eBlocker icon.....33

7.2 eBlocker Controlbar Base, Pro, Family.....33

7.3 Dashboard.....34

7.4 Tracker and Ads (Tracker- and Ad-Blocker).....35

7.5 Anon (IP-Anonymization).....37

7.6 Cloaking 37
7.7 Pause 38
7.8 Settings 38
7.9 Help 39
8 The eBlocker settings 40
8.1 General 41
8.1.1 License 41
8.1.2 Updates 41
8.1.3 Admin-Password 41
8.2 Parental Control (beta) 42
8.2.1 Activate Parental Control 42
8.2.2 User and Protection profiles 42
8.2.3 Three easy steps 43
8.2.4 Create a new user 43
8.2.5 Change settings of a user 44
8.2.6 Remove User 45
8.2.7 Create new profile 45
8.2.8 Deny access to categories of websites 47
8.2.9 Restrict internet access to certain time slots a day 48
8.2.10 Limit the maximum Internet usage per day 48
8.2.11 Assign a user to device 49
8.2.12 Controlbar for users with protection profiles 50
8.2.13 What happens if the daily internet usage time is limited? 50
8.2.14 What happens if the internet access is denied? 51
8.2.15 Add own lists to the Blacklists 53
8.2.16 Add whitelists to blacklist categories 55
8.2.17 Add own whitelist categories 56
8.2.18 Change of user through controlbar 57
8.2.19 Migration of Parental Control to eBlockerOS 1.0 58
8.3 Devices 59
8.3.1 Devices – General 60
8.3.2 Devices - General - Name 60
8.3.3 Devices - General - Activate eBlocker 60
8.3.4 Devices - Activate HTTPS 60
8.3.5 Devices - User 60
8.3.6 Devices – Blocker 61
8.3.7 Devices – Controlbar 61
8.3.8 Devices – Anonymization 61

8.3.9 Devices – Mobile 62
8.3.10 Devices – Detect new devices or remove devices from the list 63
8.4 HTTPS 63
8.4.1 HTTPS Status 64
8.4.2 SSL Certificate 65
8.4.3 SSL – HTTPS/SSL connection error 65
8.4.4 SSL - Trusted Apps 66
8.4.5 SSL - Trusted Websites 67
8.4.4 SSL – Manual diagnostic report 68
8.5 IP-Anon 69
8.5.1 Setting Up and Using the Tor Network 69
8.5.2 Set up alternative VPN network 71
8.5.3 Set up the VPN-network from Perfecty Privacy 74
8.6 DNS 79
8.6.1 DNS – Local Device names 80
8.7 Blocker 81
8.7.1 Blocker – Overview 81
8.7.2 Blocker – Advanced Features 81
8.8 System 83
8.8.1 System – Language and time zone 83
8.8.2 System - Admin-Password 83
8.8.3 System - Restart and Shutdown 84
8.8.4 System - Events 84
8.8.5 System - Diagnostics report 84
8.8.6 System – Reset 85
8.9 Network 86
8.10 eBlocker Mobile 87
9 Quick guides 90
9.1 Delete cookies, cache and browsing history in browser 90
9.1.1 Firefox 90
9.1.2 Chrome 90
9.1.3 Internet Explorer 90
10 Glossary 91
Appendix A Technical specifications (not valid for software licenses) 94
Appendix B Safety notes 94
Appendix C Manufacturer & copyright 94
Appendix D Technical support 94

Introduction

We are very pleased to know you are as concerned about your privacy as we are. We have been developing the eBlocker for more than three years in a team of experienced privacy and IT professionals. We still have a lot of ideas and are developing many more features that we are providing you monthly via updates. Thank you very much for supporting our idea of a free and private Internet by purchasing our eBlocker!

This manual explains all functions of eBlocker and will support you during commissioning. If there are still some questions left, please go to forum.eBlocker.com for answers and personal assistance.

1.1 The eBlocker Products

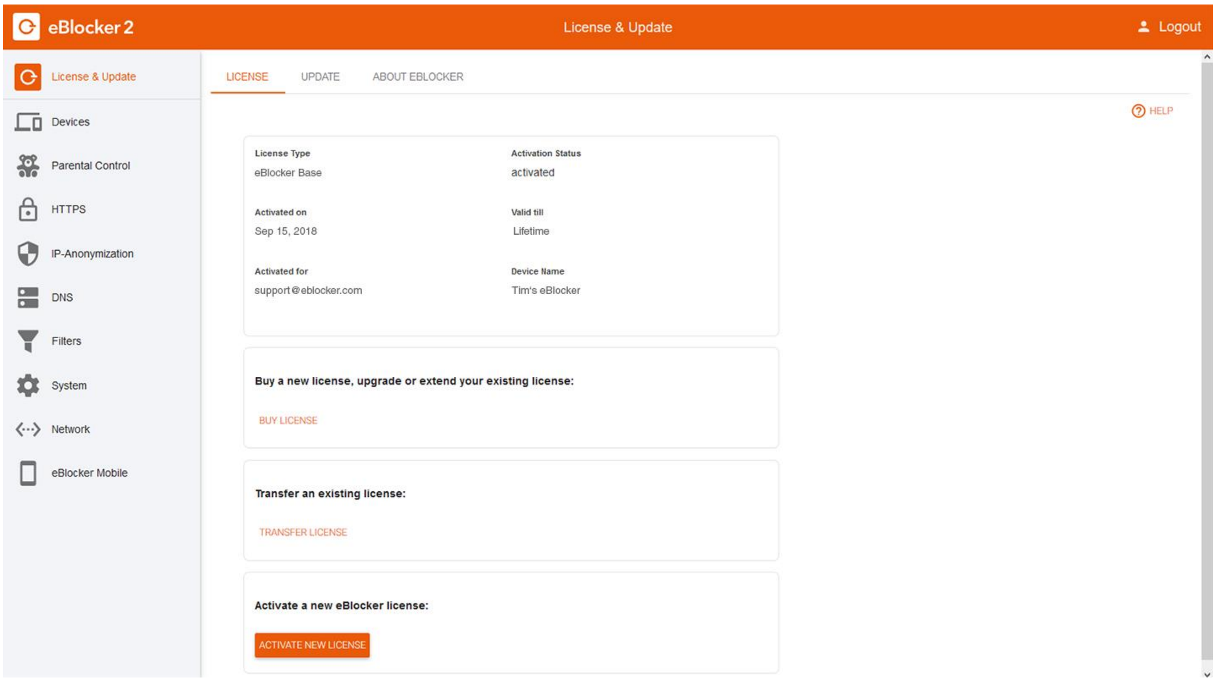
The eBlocker is available in two versions: **eBlocker Pro** and **eBlocker Family**. Both versions are based on the same technical architecture and don't differentiate in their hardware. The difference is determined by their software, after activating the license.

Whether **eBlocker Base**, **eBlocker Pro** or **eBlocker Family**: Now your privacy belongs to you again – and not to the Internet companies.

1.2 The eBlocker Versions

1.2.1 eBlocker Base

The **eBlocker Base** Is the simple protection of your privacy where your IP address is effectively anonymized when browsing. It can be upgraded to the **eBlocker Pro** or **eBlocker Family** at any time.



License Type
eBlocker Base

Activation Status
activated

Activated on
Sep 15, 2018

Valid till
Lifetime

Activated for
support@eblocker.com

Device Name
Tim's eBlocker

Buy a new license, upgrade or extend your existing license:

BUY LICENSE

Transfer an existing license:

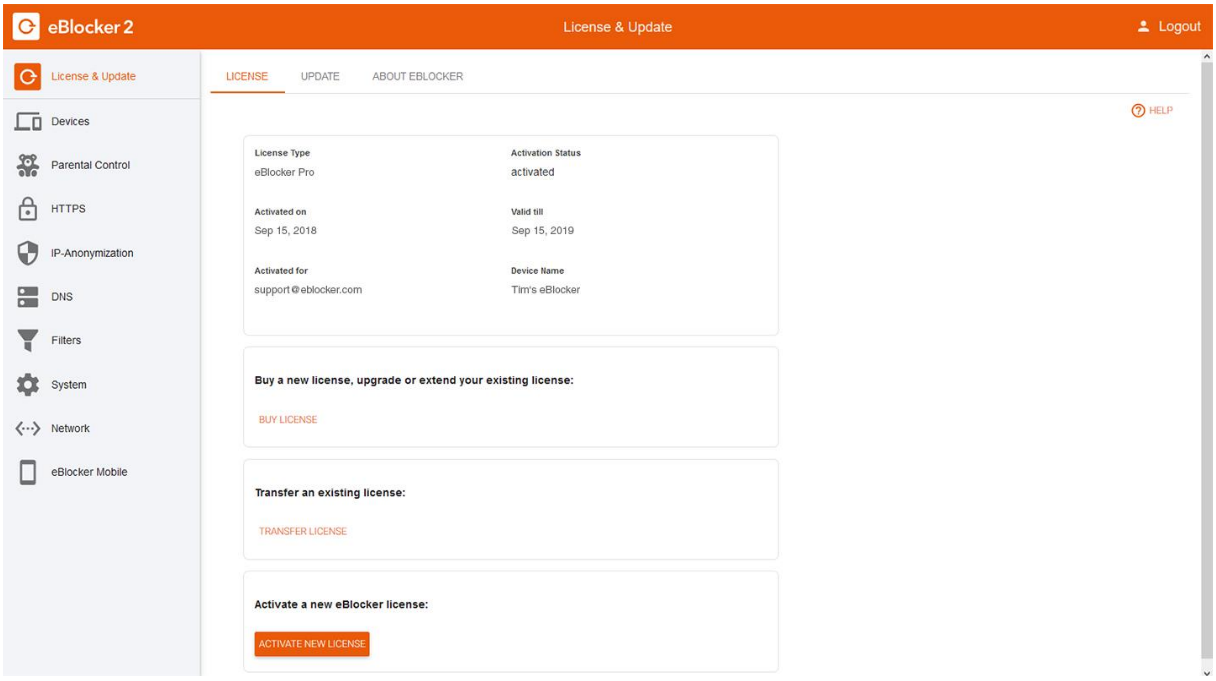
TRANSFER LICENSE

Activate a new eBlocker license:

ACTIVATE NEW LICENSE

1.2.2 eBlocker Pro

The **eBlocker Pro** includes the **eBlocker Base** features and blocks data collectors and data collecting ads on all devices and browsers - even when you are on the road. The **eBlocker Pro** can be upgraded to the **eBlocker Family** at any time.



License Type
eBlocker Pro

Activation Status
activated

Activated on
Sep 15, 2018

Valid till
Sep 15, 2019

Activated for
support@eblocker.com

Device Name
Tim's eBlocker

Buy a new license, upgrade or extend your existing license:

BUY LICENSE

Transfer an existing license:

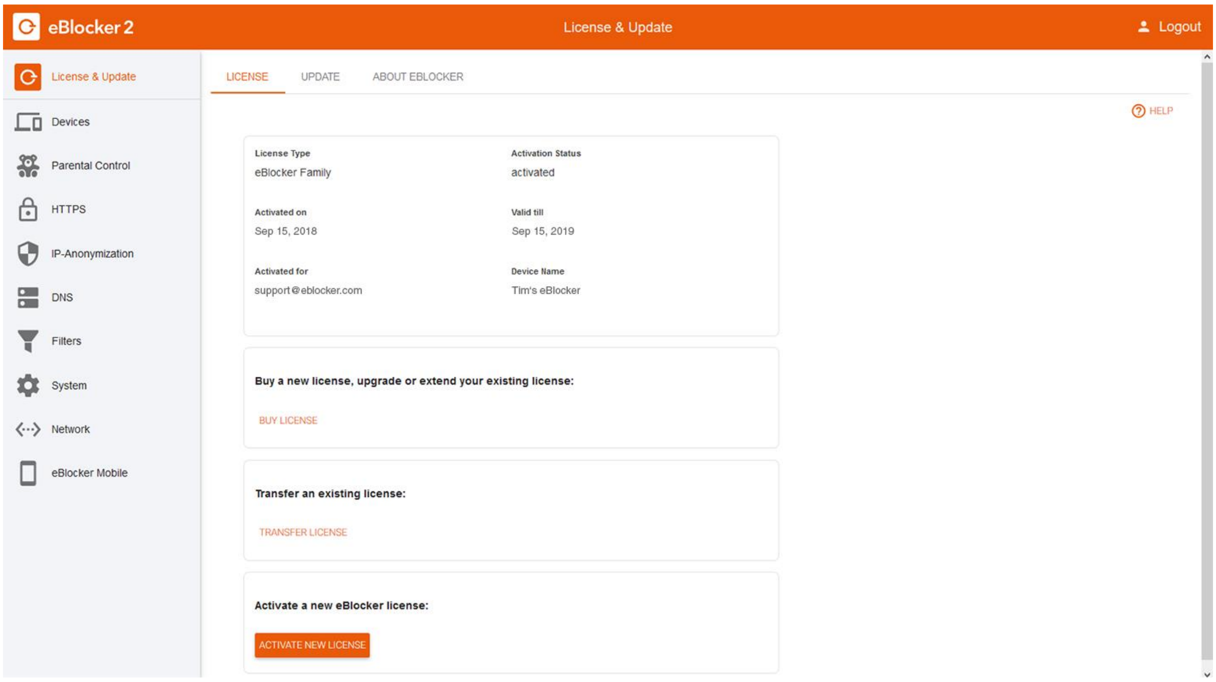
TRANSFER LICENSE

Activate a new eBlocker license:

ACTIVATE NEW LICENSE

1.2.3 eBlocker Family

The **eBlocker Family** expands eBlocker Pro with individual multi-user support and **parental controls**. Thus, eBlocker protects all family members individually – and your kids from inappropriate content.



License Type eBlocker Family	Activation Status activated
Activated on Sep 15, 2018	Valid till Sep 15, 2019
Activated for support@eblocker.com	Device Name Tim's eBlocker

Buy a new license, upgrade or extend your existing license:

BUY LICENSE

Transfer an existing license:

TRANSFER LICENSE

Activate a new eBlocker license:

ACTIVATE NEW LICENSE

The three eBlocker versions have the same hardware and are based on the same software. The features are available in the settings depending on the eBlocker version, or the feature points out for which eBlocker version it is available for.

2 Commissioning

By following this user manual, you will be able to set up your eBlocker in no time.

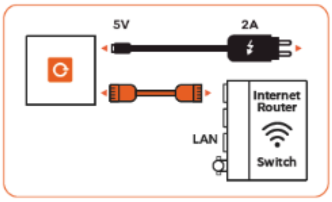
Please follow the steps to put your device in operation.

In only three steps your eBlocker is ready for use:

1. Connection

First, connect your eBlocker to your router or switch, with the **orange LAN cable**.

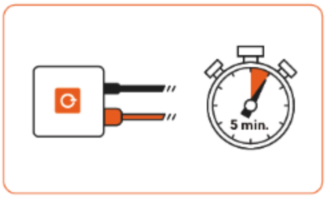
Then connect your eBlocker **with the adapter cable** and the power supply.



Automatic configuration

Wait for 5 minutes until your eBlocker has automatically configure itself.

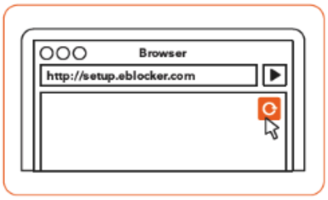
Start an Internet browser and go to: http://setup.eblocker.com



Start

The eBlocker icon appears at the top right of your browser. With a click on the icon, you will be lead to the so called “controlbar”, in which you can view the most important information about the page you are currently visiting. You are able to customize the eBlocker settings here.

The network link leads you to the network setup wizard. If the icon does not appear, you can find help in section [0](#).



3 Activation

Please have your serial-number of your eBlocker as well as the license key and your email address ready for the activation.

Find the **serial number** on the type plate at the bottom of the package and at the bottom of the device. It has the format “SNXXXXXXXX”.

The **license key** is placed on the **license card**, which is included in the device packaging. Please use a valid email address in the activation process. If you want to transfer your eBlocker license to another device sometime, your email address will also be needed then.

4 Use eBlocker optimally

4.1 Summary

After the activation process is done, we recommend you the following steps, so you can use eBlocker as optimal as possible:

- Delete the cookies, cache and browsing history in all used browsers.
- Activate SSL (HTTPS-Support) in your eBlocker.
- Adopt eBlocker's certificate into your operating system and if necessary, in the browsers with their own certificate store as described in section 6.2.
- Activate possible exception lists for specific apps, so eBlocker can't protect these apps from third parties anymore.
- You may define additional exceptions for encrypted connections (SSL) – for example, for websites in which eBlocker should not be active, like online-banking sites.

Find all detailed steps explained in the following.

4.2 Deleting cookies, cache and browsing history

eBlocker automatically blocks all data collecting cookies or other elements that identify you.

However, your browser has probably collected numerous tracking cookies of different providers already. Therefore we recommend to **delete all your cookies** at first, so the trackers "can lose their track".

You can read more about how to delete cookies in your respective browser in section 9.1.

4.3 Activate support for HTTPS/SSL encrypted connections

How you can activate support for HTTPS/SSL encrypted connections, we describe in section **Fehler! Verweisquelle konnte nicht gefunden werden.**.

4.4 Activate exceptions for apps

How you can activate exceptions for apps, we describe in section **Fehler! Verweisquelle konnte nicht gefunden werden.**.

4.5 Final recommendation

We have developed our eBlocker very carefully and are constantly improving it. Nevertheless, our eBlocker is no "magic pill" for privacy that works under all circumstances. Apps in particular which are installed in your device/OS natively, represent an increased risk for your privacy. Therefore we recommend to **not use any apps at all** if possible.

Apps are very common today for accessing Internet services. However, they involve a greater risk for your privacy, as when you use the same service through a browser. Why you should avoid apps to protect your privacy, we explain below:

- **Attack into your privacy**

Apps such as Facebook, WhatsApp or Twitter can have a direct access to your device and use their own communication protocols, which cannot be protected by your eBlocker.

- **Transfer of malware**

Even the transfer of malicious software represents great danger. App stores do not only provide safe programs, but increasingly apps, that are infected with malware. These infected programs can transmit mobile data (e.g. contact details) unnoticed and without authorization or even send fee-based SMS to service numbers.

Use exceptions sparingly

Some apps are only compatible with eBlocker, if they are not monitored by eBlocker. Corresponding exception lists for these apps can be activated in the settings by clicking on “Apps”. They will not be analyzed by Blocker anymore. Please note that your privacy heads to the danger zone with every exception you make. Data can be collected without you noticing it.

5 If something may not work

Despite of the simple Plug & Play solution of eBlocker, some incompatibilities may appear that can have different causes. We have summarized some options below, which can help you in stressful times.

5.1 Connection- and network problems

- **Individual setup**

Your eBlocker is setup in the automatic network mode by default with initial connection. This mode is compatible with most network devices. Should any connecting errors occur or your network slows down, you can setup your eBlocker individually with only a few clicks. By setting it up individually, all network problems will normally be resolved immediately. How you can setup your eBlocker individually, we describe in section 8.9.

5.2 A website is not displayed

If the eBlocker usually works but errors occur on certain websites, we have summarized some tips for help:

- **Pause eBlocker**

Click on the eBlocker icon in the upper right corner of your browser window. With the "Pause" feature you can pause the eBlocker for a few minutes for the device you are using. Try to reload the according website afterwards. If the pause feature worked and you visit this website frequently, we recommend adding an exception for this website.

- **Add exceptions (Whitelisting)**

Available for **eBlocker Pro** and **eBlocker Family**

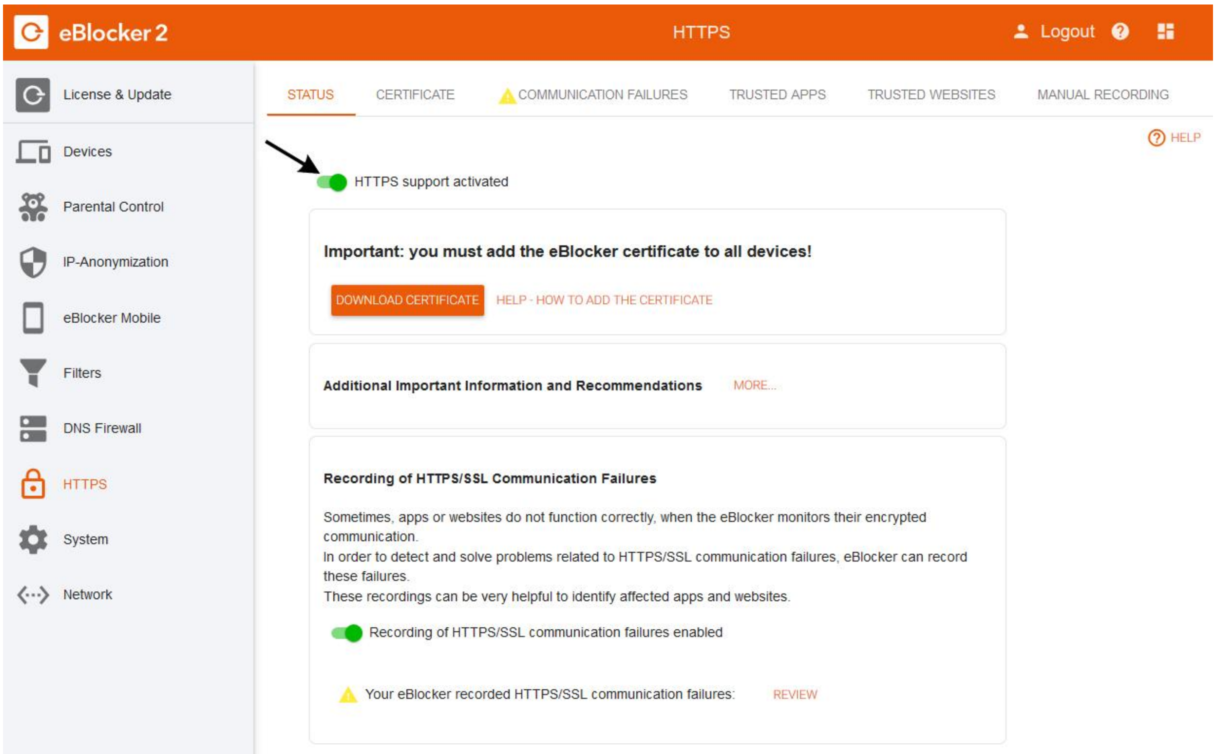
If you cannot see a website or are blocked from viewing the website, you can add exceptions to this website. How to add these exceptions is described in chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**.

- **Disable HTTPS completely or for individual devices**

Available for **eBlocker Pro** and **eBlocker Family**

In rare cases, individual HTTPS-loaded websites or apps may not be compatible with eBlocker. You can easily check this by disabling the HTTPS feature for the eBlocker or only for the current device.

To completely disable the HTTPS feature, open the eBlocker Controlbar. Go to the settings and then click on "HTTPS". Deactivate the HTTPS support feature by clicking on the orange slide switch next to the words "HTTPS support".



HTTPS support activated

Important: you must add the eBlocker certificate to all devices!

Additional Important Information and Recommendations

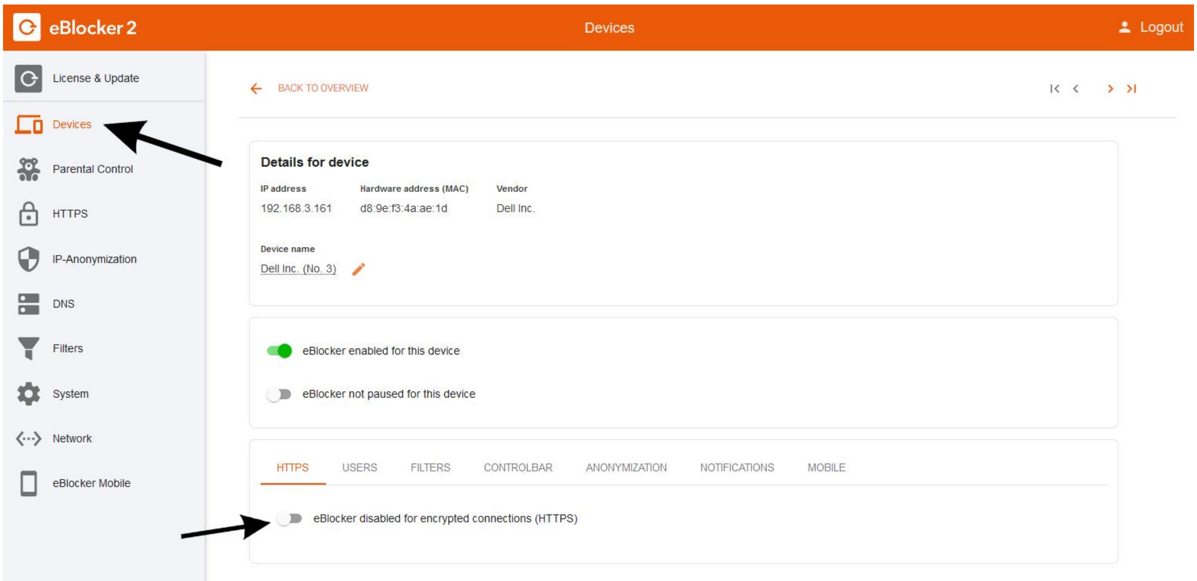
Recording of HTTPS/SSL Communication Failures

Sometimes, apps or websites do not function correctly, when the eBlocker monitors their encrypted communication.
In order to detect and solve problems related to HTTPS/SSL communication failures, eBlocker can record these failures.
These recordings can be very helpful to identify affected apps and websites.

Recording of HTTPS/SSL communication failures enabled

Your eBlocker recorded HTTPS/SSL communication failures:

To disable the HTTPS function on a specific device only, please proceed as follows. In Preferences, click Devices. Locate the device on which you want to disable the HTTPS feature. Your current device is always displayed first on the list.



Details for device

IP address	Hardware address (MAC)	Vendor
192.168.3.161	d8:9e:f3:4a:ae:1d	Dell Inc.

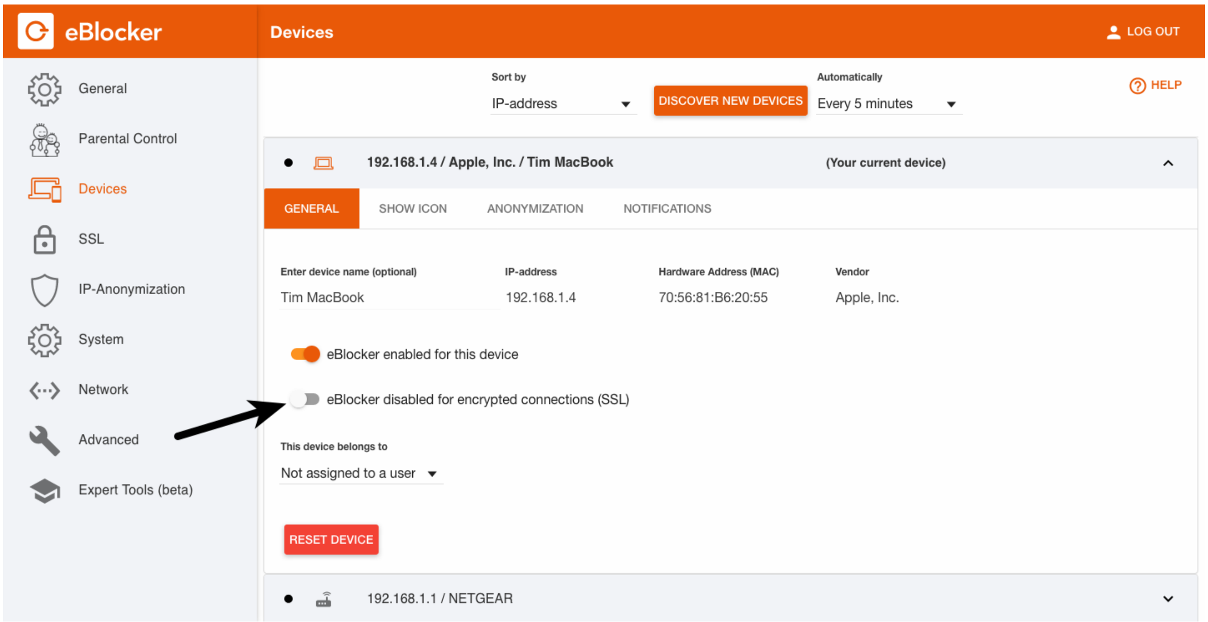
Device name
Dell Inc. (No. 3)

eBlocker enabled for this device

eBlocker not paused for this device

eBlocker disabled for encrypted connections (HTTPS)

Open the settings for the desired device by clicking on the corresponding line and deactivate HTTPS for the device with the slide switch.



Sort by: IP-address

Automatically: Every 5 minutes

● 192.168.1.4 / Apple, Inc. / Tim MacBook (Your current device)

Enter device name (optional)	IP-address	Hardware Address (MAC)	Vendor
Tim MacBook	192.168.1.4	70:56:81:B6:20:55	Apple, Inc.

eBlocker enabled for this device

eBlocker disabled for encrypted connections (SSL)

This device belongs to: Not assigned to a user

● 192.168.1.1 / NETGEAR

■ **Disable HTTPS for individual websites or apps**

If the problem has been solved by disabling the HTTPS feature, the corresponding web page can be permanently added to an exception list.

First check whether there is already a predefined list of exceptions for the app in question and whether the corresponding website appears in this exception list, by clicking on the menu HTTPS > tab “Trusted Apps”. If so, activate the exception list with its check box.

5.3 The eBlocker icon does not displayed on all devices

If your eBlocker works fine in general, but the eBlocker icon is not showing on all devices, we have summarized some tips that can help.

■ **Activate device**
Open your browser window and click on the eBlocker icon. Go to “Settings” and then select “Devices”. On the right side you will see a list of all devices connected to the eBlocker in your home network. Check whether your device, its manufacturer or IP address is displayed. For information on how to activate your device, see section 8.3.3.

■ **Display the eBlocker icon**
Open your browser window and click on the eBlocker icon. Go to “Settings” and then select “Devices”. On the right side you will see a list of all devices connected to the eBlocker in your home network. Click on the IP address or its manufacturer and see if the eBlocker icon is displayed for your device. You can read how to activate or deactivate the eBlocker icon for a device in chapter 0.

5.4 The eBlocker icon is not showing on any device

■ **Reboot eBlocker**

If you have connected your eBlocker for the first time and you have visited http://setup.eblocker.com but still no icon shows after 5 minutes waiting: reboot your eBlocker. Disconnect the device from the power supply and wait for 30 seconds. After 30 seconds connect your eBlocker to the power supply again.

- **Delete cookies and cache and reload website**

Delete the cookies and cache of your browser or press and hold the shift key while clicking on browser icon „reload page". You can read in section 4.1 how to delete cookies.

Please note that your eBlocker needs 5 minutes after initial connection to configure itself automatically.

- **Activate device**

Make sure that your device appears under „Settings/Devices" and is activated. How you can activate devices, is described in section 8.3. If your device is activated, but the icon is not showing, please read section 5.3.

5.5 Removing common problems

- **Plug in your cable correctly**

Please check your scope of supply with your delivery. Make sure that your delivery is complete and check if you are really *only* using the accessory cable and the power supply. Test if the cables are plugged in *correctly and fully inserted*.

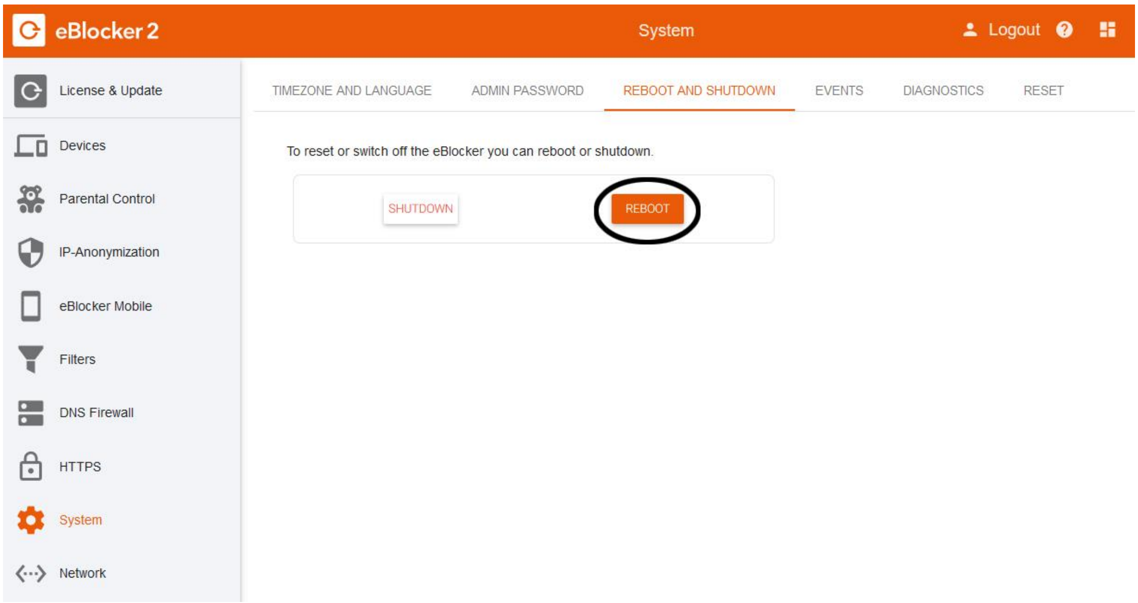
- **Plug in cable into the right ports**

Please make sure that the LAN cable is really plugged into the „LAN" port and the power supply is plugged into the "POWER" port. The „HDMI" and "USB" ports are for future enhancements and currently not in function.

Please note that some routers have limited LAN ports that cannot be used by the eBlocker. These port are LAN1 or LAN4/LAN5 most of the time. Please connect your eBlocker with one of the other ports of your router.

- **Reboot eBlocker**

Open your browser and click on the eBlocker icon at the top right of your browser. Go to Settings and click on "System" afterwards.



To reset or switch off the eBlocker you can reboot or shutdown.

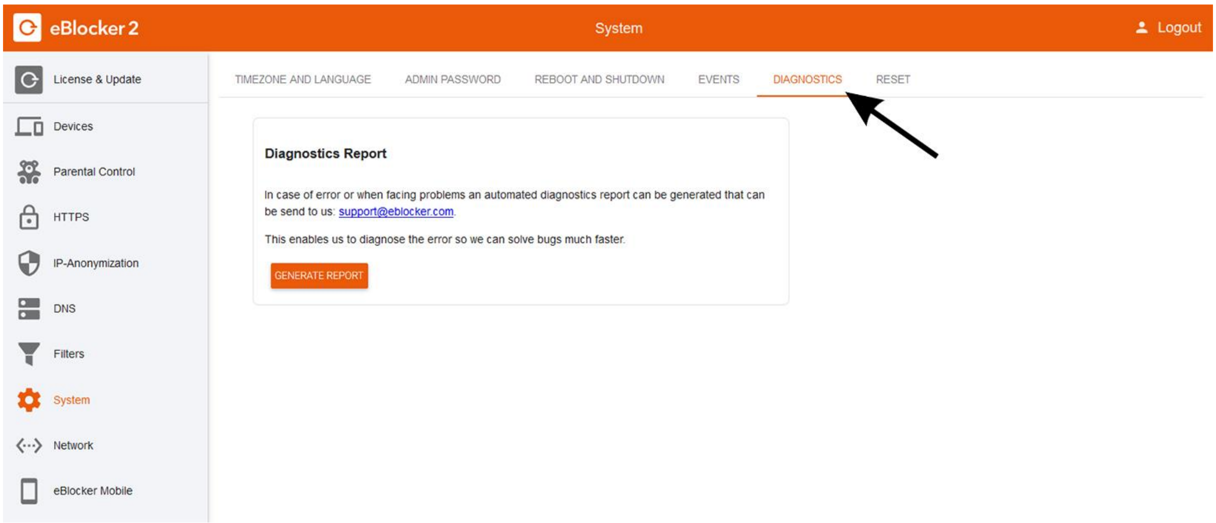
The button „Reboot and Shutdown“ is already highlighted in orange. Click on “Reboot” and your eBlocker will reboot itself.

If the eBlocker settings cannot be accessed, you can reboot your device by disconnecting your eBlocker from your power supply. Please wait for 30 seconds before reconnecting your device to the power supply.

Please note that your eBlocker needs 5 minutes to detect the network and configuring itself after rebooting.

- **Send diagnostic report to support team**

In case of error or problems, you can create an automatic diagnostic report that you can send to us (section Appendix D). Through the diagnostic report, we will know in which state your device is in and thus a quick solution can be found.



Diagnostics Report

In case of error or when facing problems an automated diagnostics report can be generated that can be send to us: support@eblocker.com.

This enables us to diagnose the error so we can solve bugs much faster.

- **Reboot router**

Shut down your router and reboot it afterwards. Please consider the user manual of your router. Usually it only requires to disconnect the router from the power supply and connecting it right back in after a short time.

5.6 Some apps don’t work

Unlike normal browsers, apps have more access options on your device. While most browsers and websites will work fine with your eBlocker, some app incompatibilities may occur.

Especially if the eBlocker is also activated for encrypted connections (HTTPS), problems can occur with individual apps. Usually the problems can be easily solved if the corresponding websites with which the app communicates via HTTPS (SSL) are excluded from the eBlocker analysis.

There are already prepared exception lists for some of the most popular apps, which you can view and activate in the "HTTPS" menu > "Trusted Apps" tab.

However, you can also define your own exception lists for other apps or edit and supplement the existing exception lists.

Especially with apps it is not always easy to find out which websites are actually addressed by the app. To facilitate analysis, the eBlocker can also automatically display connection errors in the "HTTPS" > "HTTPS/SSL Connection Errors" tab. The eBlocker also provides an "expert tool" for recording and evaluating connections and makes suggestions as to which websites should be included in the list of exceptions. This expert tool is described in section **Fehler! Verweisquelle konnte nicht gefunden erden.**.

But don't worry, if you're not an expert, please post a short message in our forum (forum.eblocker.com). Just let us know which app or app feature doesn't work with eBlocker. Perhaps another member has already solved exactly the same problem and can help you.

Please note that eBlocker cannot protect you when using app exception lists on the respective websites. Even if you do not access it with the app but with a web browser.

Please also read our recommendations in section 4.6 in connection with apps.

5.7 The eBlocker completely stopped operating

Please make sure to activate your DHCP server.

Remove your eBlocker from your network and disconnect the eBlocker from the power supply. Now remove all other devices (your computer, notebook, smartphone, etc.) from your network and connect them again to update the DHCP lease. You can also update your DHCP lease for most of the devices, in the network settings. Your devices are now connected to the Internet again.

Remove the network cable from your computer and deactivate the Wi-Fi, if needed. Connect the eBlocker with the network cable to your computer and connect the eBlocker to the power supply. Now wait for 5 minutes. Call the emergency-IP of the eBlocker: http://169.254.94.109:3000 to get to the eBlocker settings.

Go to „Network“ and set it to „automatic“. Save the settings afterwards. The eBlocker might reboot now. Wait for the reboot and go to the eBlocker settings again. Click on „system“ and shutdown your eBlocker. Remove the device from your computer and from the power supply. Don’t forget to reconnect your computer to the network and/or to reactivate your Wi-Fi. Now connect your eBlocker to your router and to your power supply again.

5.8 More help: Our forum and support

Many useful answers to common questions can be found in our forum at http://forum.eBlocker.com

We are pleased to assist you via email as well (see Appendix D).

6 Tips and Tricks

6.1 The individual setup – eBlocker overtaking the DHCP server

Available for **eBlocker Base**, **eBlocker Pro** and **eBlocker Family**

You have connected the eBlocker and are now having trouble with your network?

This may be because you are using a router that is not immediately compatible with the plug & play feature of the eBlocker.

However, you do not have to give up the protection of the eBlocker and can put the eBlocker into operation in just four simple steps.

If you do not understand a term, you will find explanations for all technical terms in the glossary of our manual.

- Find out how to deactivate the DHCP server of your router through the detailed information in your router manual.
- Click on “Network” in your eBlocker settings and go to the network assistant.
- Read the preparations carefully and click on the button “Next”.
- Read the process carefully and click on the button “Next”.
- Now please write down or print out the displayed settings. After doing so, click on the button “Next”.
- Confirm all three steps and click on “Perform and Reboot”.

Your eBlocker is fully configured after the reboot. Now your router is next to be converted.

- Log into your router as an administrator.
- You have to change the settings for some routers (e.g. from standard to extended).
- Deactivate the DHCP server of your router and save the settings.
- Finally renew the so called DHCP lease for all active client devices that are located in your network (computer, notebook, smartphone, etc.).

It is important to renew the DHCP lease, so all client devices will not use the old network information. You will receive the new DHCP lease easily through disconnecting the network connection from the client devices, for example. Some devices also provide the button „Update DHCP lease“ in their network settings.

Note: If you want to undo this setting you have to activate the DHCP server in your router first. Deactivate the DHCP server of your eBlocker afterwards or set your eBlocker to “automatic” in the network settings.

6.2 Adding the eBlocker certificate

We recommend our customers to add the eBlocker certificate into their operation system first. Most of the browsers and programs need to use the eBlocker certificate to have access to HTTPS sites. Several programs have their own certificate stores. How the eBlocker certificate is inserted into these certificate stores, we describe in this segment.

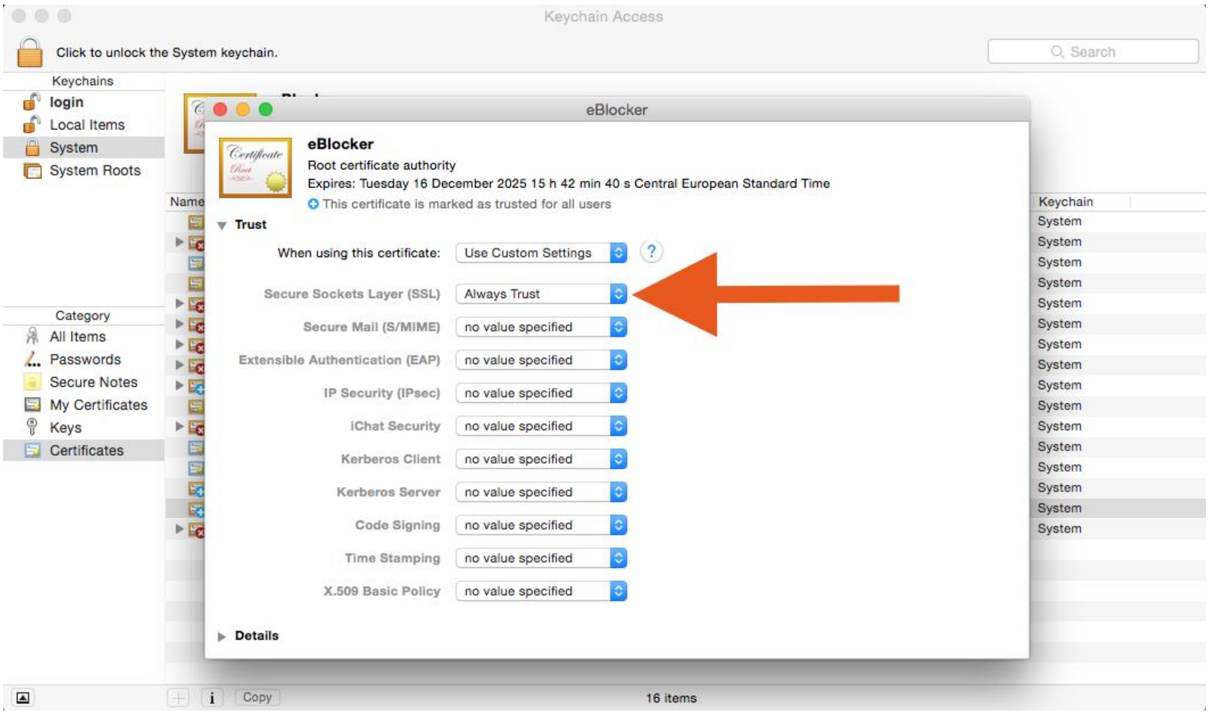
6.2.1 macOS

You have added the certificate with only a few clicks. Open the Safari browser.

Open the eBlocker HTTPS configuration page..

Click on the button *add certificate*, to save the eBlocker 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.



eBlocker

eBlocker
Root certificate authority
Expires: Tuesday 16 December 2025 15 h 42 min 40 s Central European Standard Time
This certificate is marked as trusted for all users

Trust

When using this certificate:	Use Custom Settings
Secure Sockets Layer (SSL)	Always Trust
Secure Mail (S/MIME)	no value specified
Extensible Authentication (EAP)	no value specified
IP Security (IPsec)	no value specified
iChat Security	no value specified
Kerberos Client	no value specified
Kerberos Server	no value specified
Code Signing	no value specified
Time Stamping	no value specified
X.509 Basic Policy	no value specified

Details

The eBlocker certificate has now been added into macOS. Most of the browsers and programs can have access to the eBlocker certificate now.

Here a list of a few common browsers you can have access to the eBlocker controlbar on HTTPS sites with.

- Safari
- Google Chrome
- Opera
- Vivaldi
- Yandex

The following browsers have their own certificate store. The eBlocker certificate has to be inserted into the according certificate store.

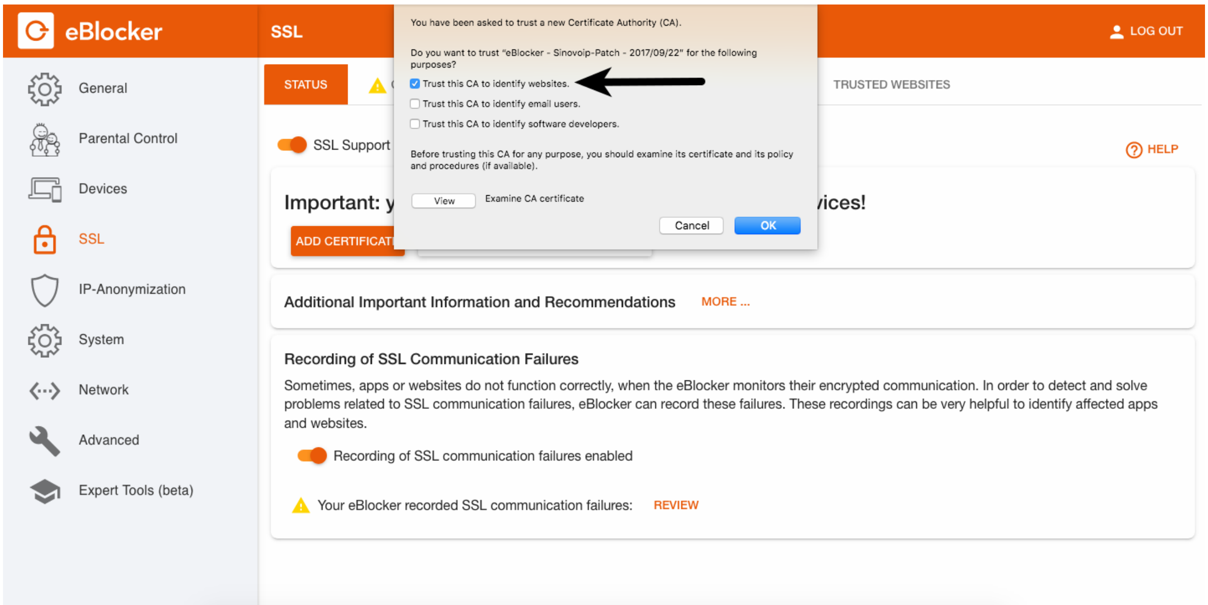
- Firefox
- Cliqz (based on Firefox)
- Seamonkey
- Thunderbird (email program)

Firefox, Cliqz and Seamonkey

Open the eBlocker SSL configuration site.

Click on the button *add certificate*.

Make sure that the first checkbox ‚*Trust this CA to identify websites’* is selected (see image below).



You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "eBlocker - Sinovoip-Patch - 2017/09/22" for the following purposes?

☑ Trust this CA to identify websites.
□ Trust this CA to identify email users.
□ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Recording of SSL Communication Failures

Sometimes, apps or websites do not function correctly, when the eBlocker monitors their encrypted communication. In order to detect and solve problems related to SSL communication failures, eBlocker can record these failures. These recordings can be very helpful to identify affected apps and websites.

Recording of SSL communication failures enabled

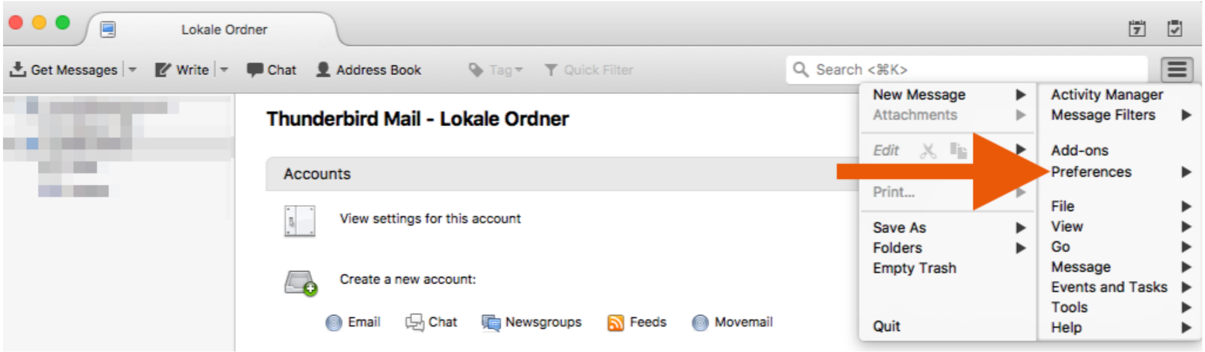
Your eBlocker recorded SSL communication failures: REVIEW

Click on *OK* to insert the eBlocker certificate in Firefox.

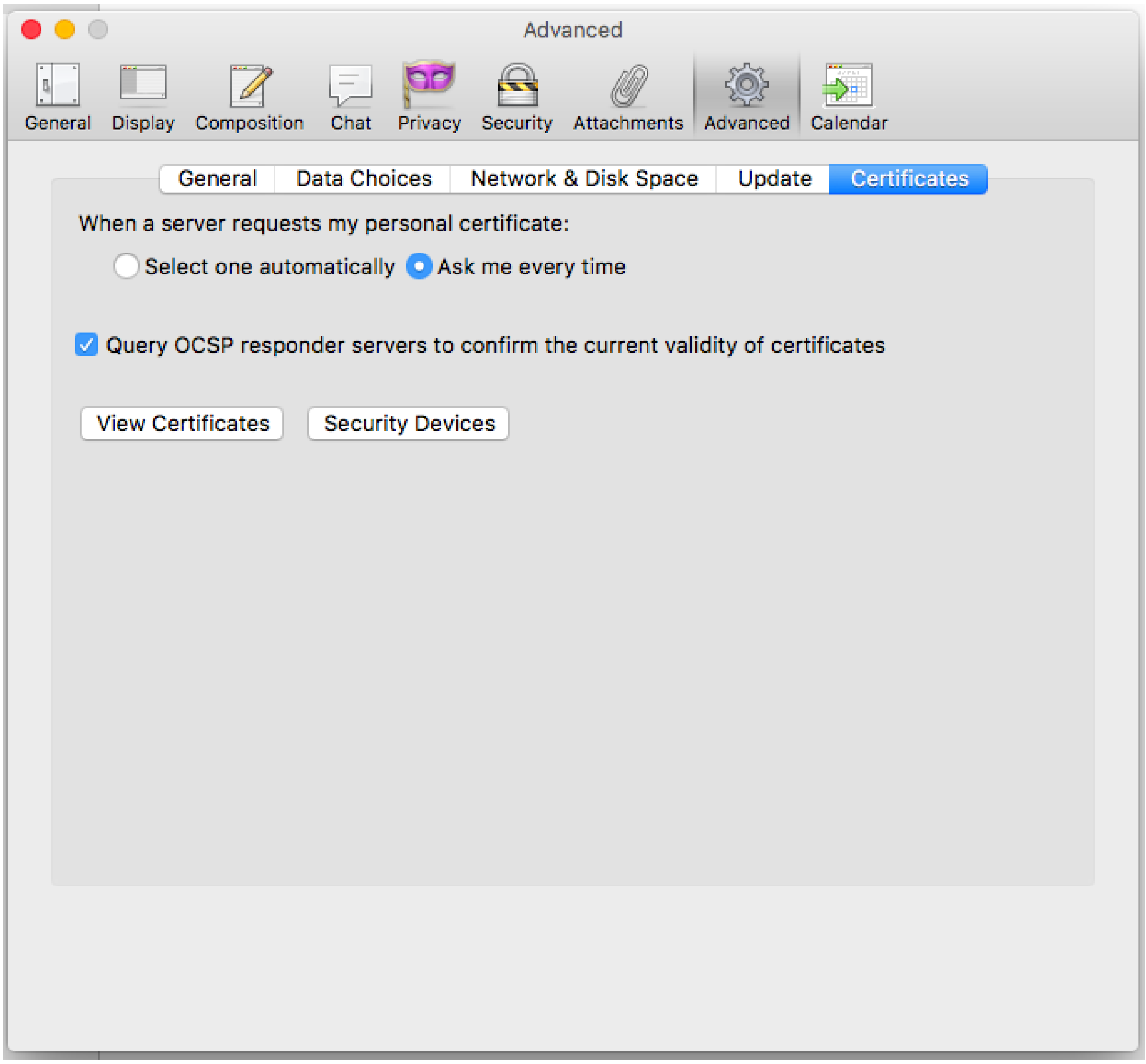
You can see the eBlocker controlbar now on HTTPS sites with the Firefox, Cliqz or Seamonkey browser.

Thunderbird (email program)

Go to the menu and click on *Preferences*.



Go to Advanced and click on View Certificates.

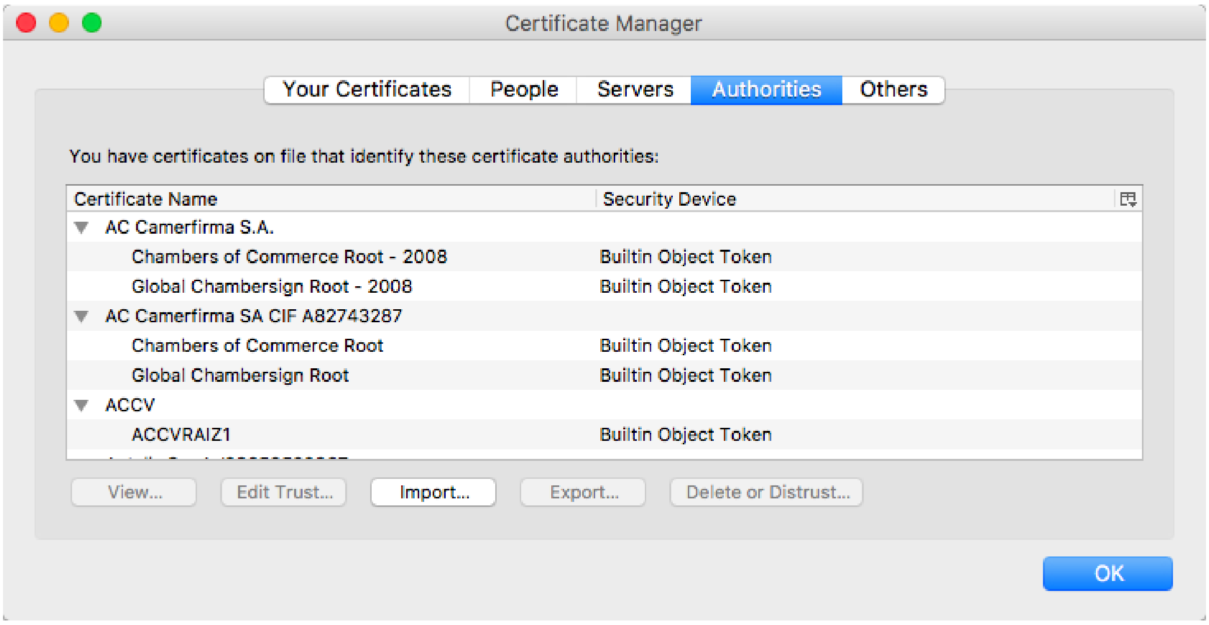


When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

☑ Query OCSP responder servers to confirm the current validity of certificates

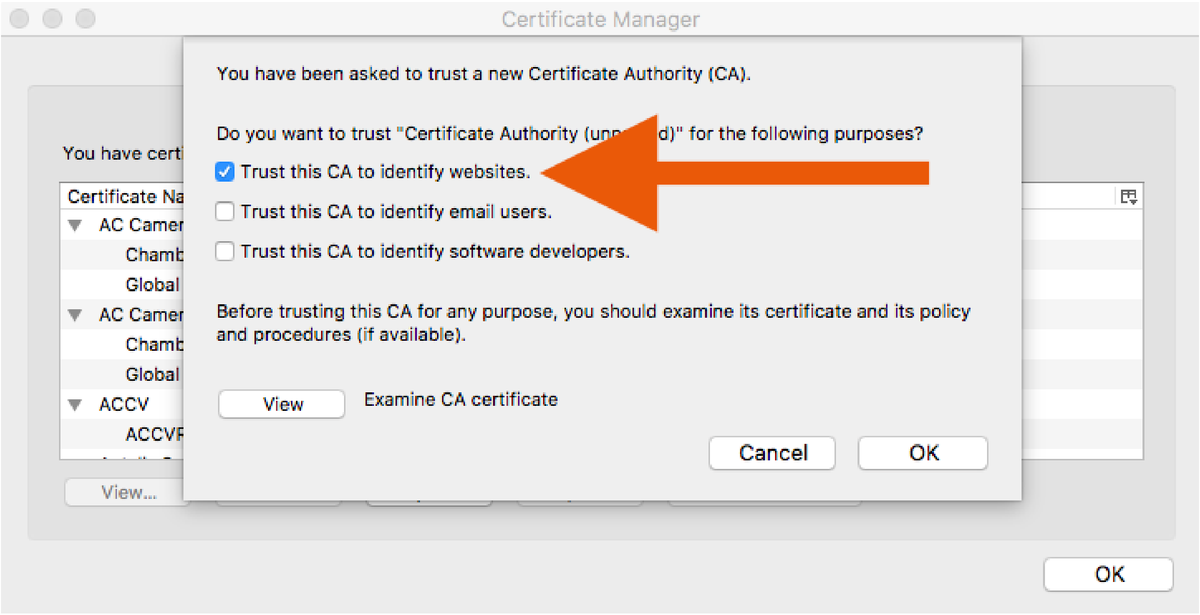
After the Certificate Manager opens, click on *import* and choose the eBlocker certificate from the downloads directory.



You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
▼ AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
▼ AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token
▼ ACCV	
ACCVRAIZ1	Builtin Object Token

Open the eBlocker certificate and make sure that the first checkbox ‚*Trust this CA to identify websites*' is selected. Confirm with *OK*.



You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "Certificate Authority (unn d)" for the following purposes?

☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

□ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Examine CA certificate

Confirm the Certificate Manager and the settings with *OK*.

The certificate is now inserted into the Thunderbird email program.

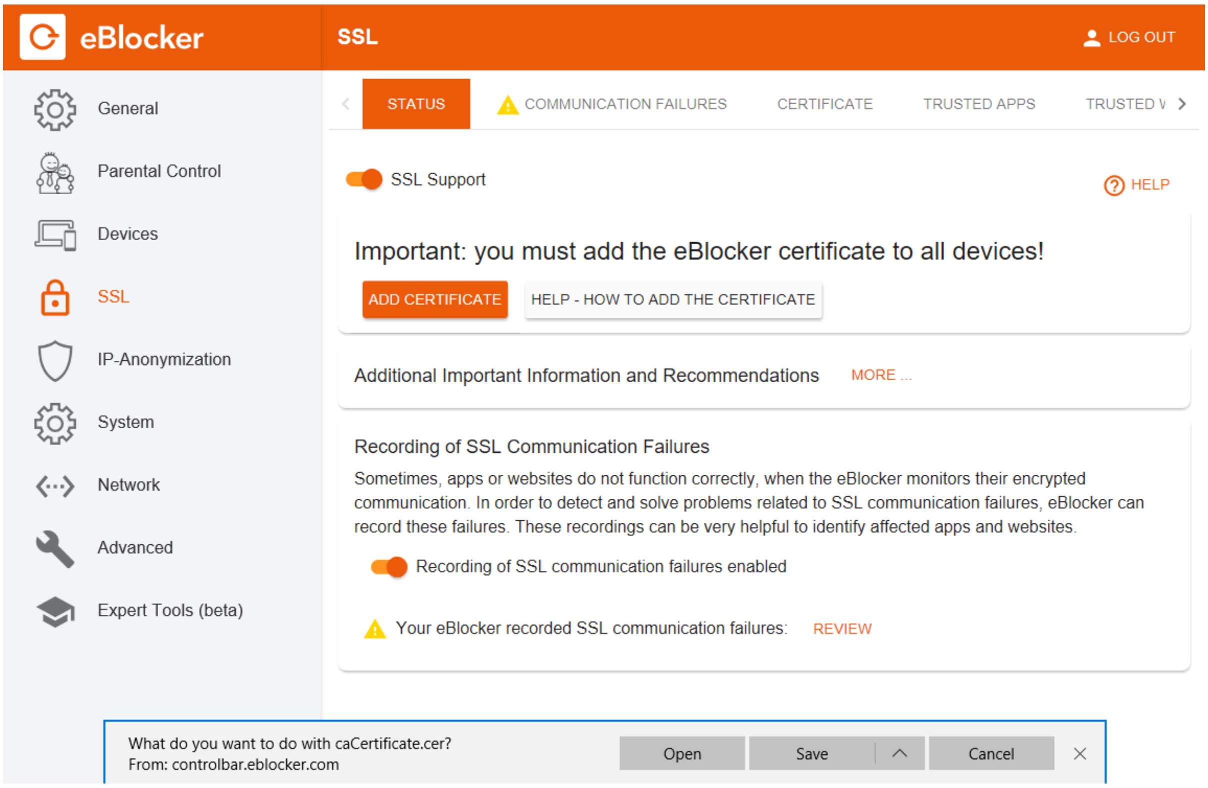
6.2.2 Windows

You have inserted the certificate with only a few clicks. Please use the Microsoft Internet Explorer or the Edge browser.

Open the eBlocker SSL configuration site.

Click on the button add certificate.

After the dialog appears, go to save and then click on open.



SSL Support

Important: you must add the eBlocker certificate to all devices!

Additional Important Information and Recommendations

Recording of SSL Communication Failures

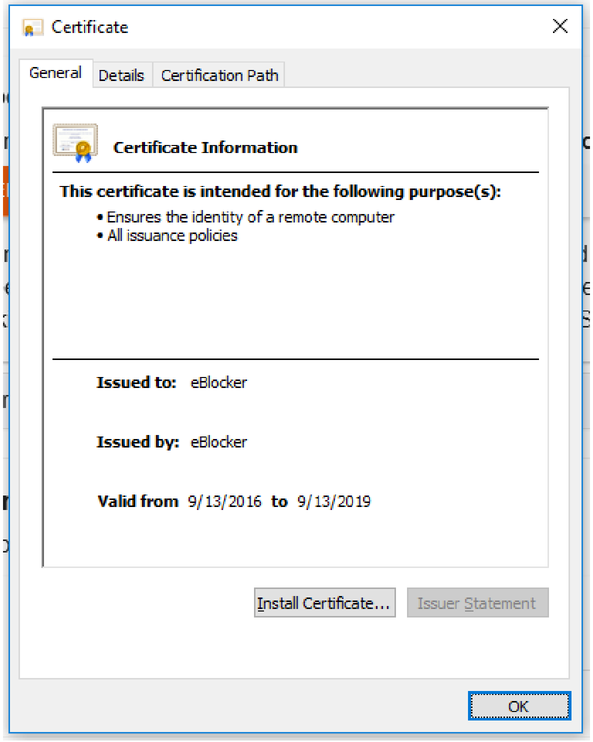
Sometimes, apps or websites do not function correctly, when the eBlocker monitors their encrypted communication. In order to detect and solve problems related to SSL communication failures, eBlocker can record these failures. These recordings can be very helpful to identify affected apps and websites.

Recording of SSL communication failures enabled

Your eBlocker recorded SSL communication failures:

What do you want to do with caCertificate.cer?
From: controlbar.eblocker.com

Click on Install Certificate.



Certificate Information

This certificate is intended for the following purpose(s):

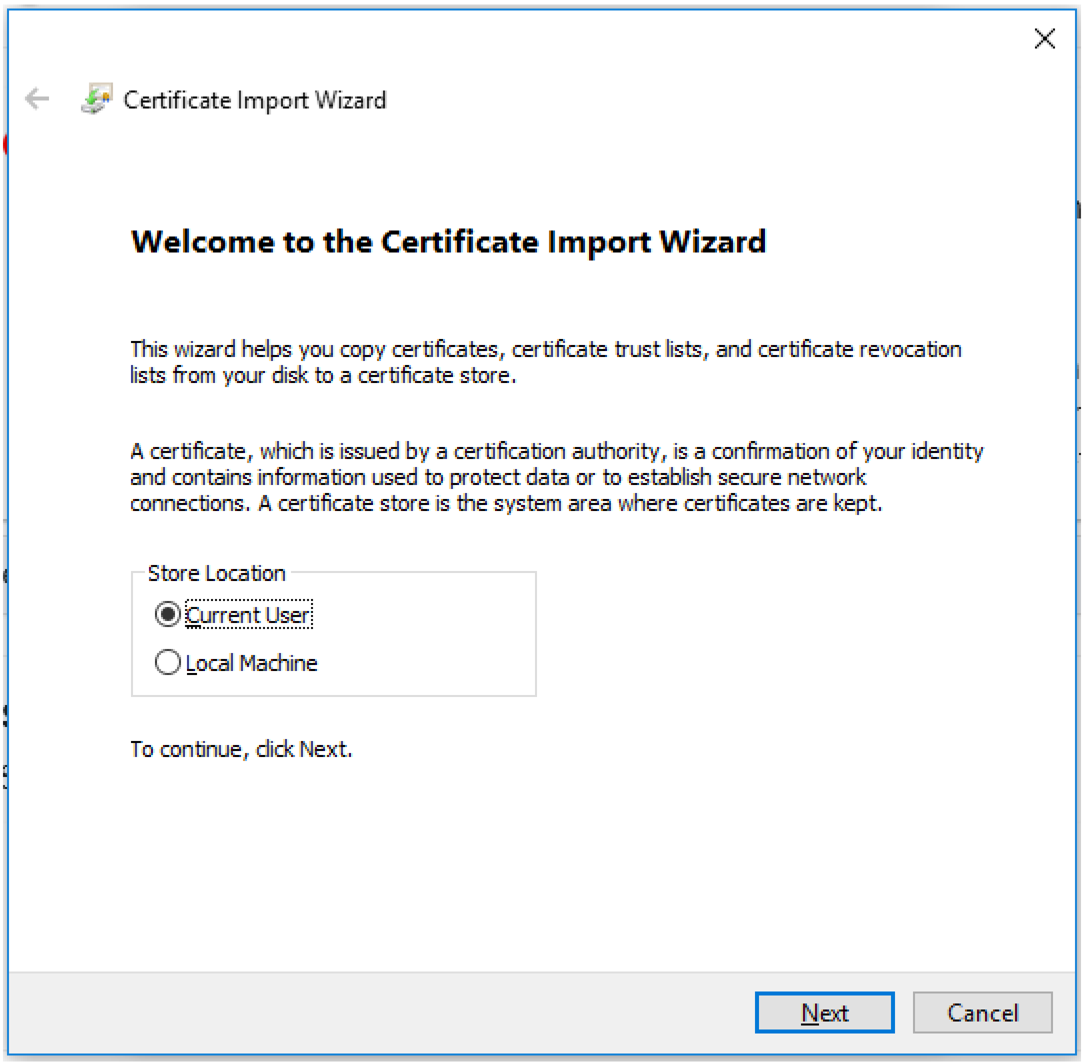
- Ensures the identity of a remote computer
- All issuance policies

Issued to: eBlocker

Issued by: eBlocker

Valid from 9/13/2016 to 9/13/2019

The Certificate Import Wizard opens. Click on *Next*. Go to *safe all certificates into the following storage* and click on *browse* afterwards.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

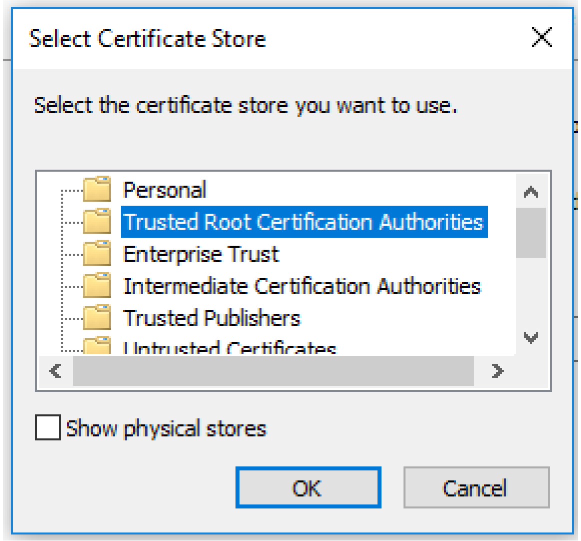
Store Location

● Current User

○ Local Machine

To continue, click Next.

Choose the second register *Trusted Root Certification Authorities* and confirm this process with *OK*.

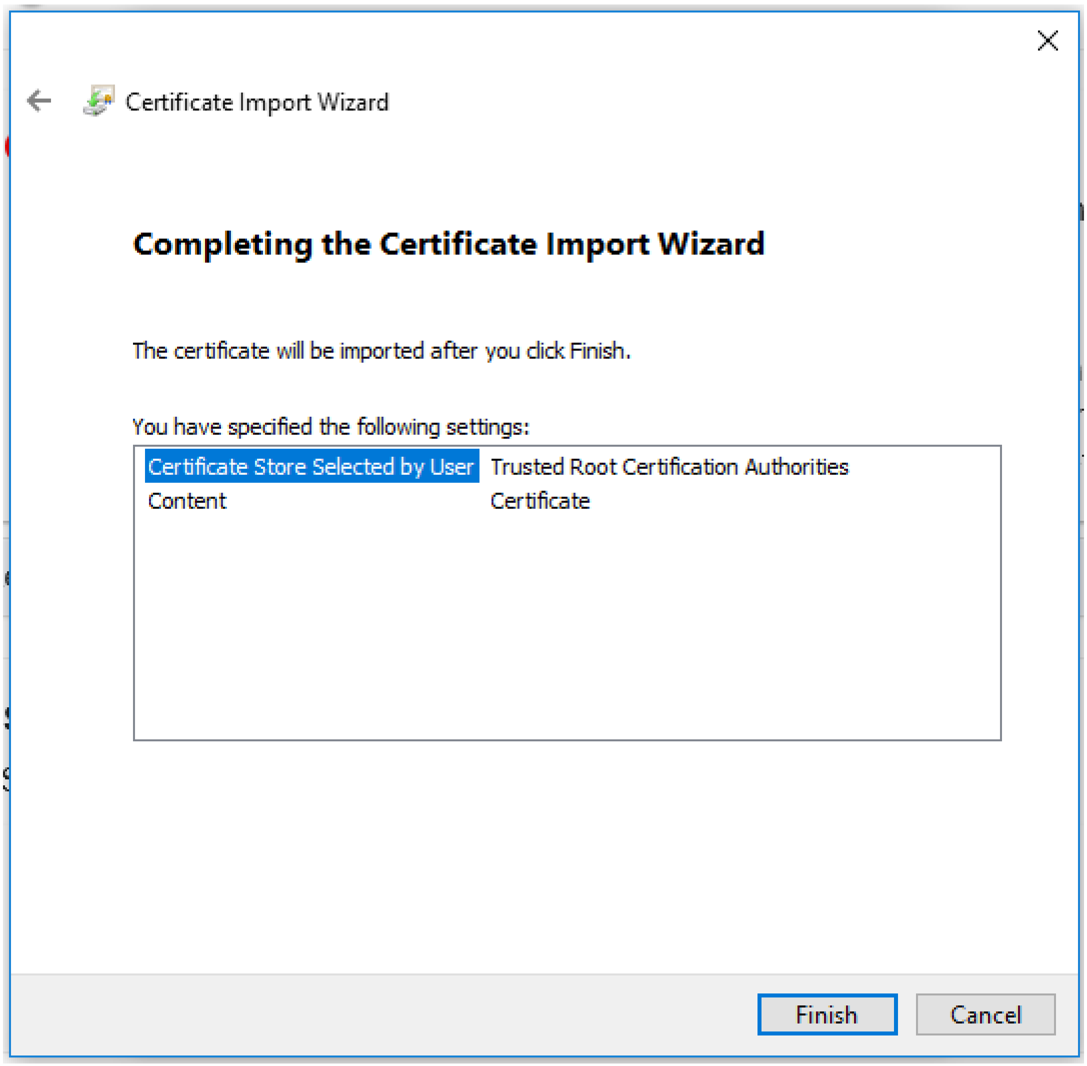


Select Certificate Store

Select the certificate store you want to use.

Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates

□ Show physical stores



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

Click on *Next* in the Certificate Import Wizard and confirm the process with *Finish*.

Confirm the following safety warning with *Yes*.

The eBlocker certificate is now inserted into Windows. Most of the browsers and programs can have access to the eBlocker certificate.

Here a list of a few common browsers you can have access to the eBlocker controlbar on HTTPS sites with.

- Microsoft Internet Explorer
- Microsoft Edge
- Google Chrome
- Opera
- Vivaldi
- Yandex

The following browsers have their own certificate store. The eBlocker certificate has to be added to the according certificate store.

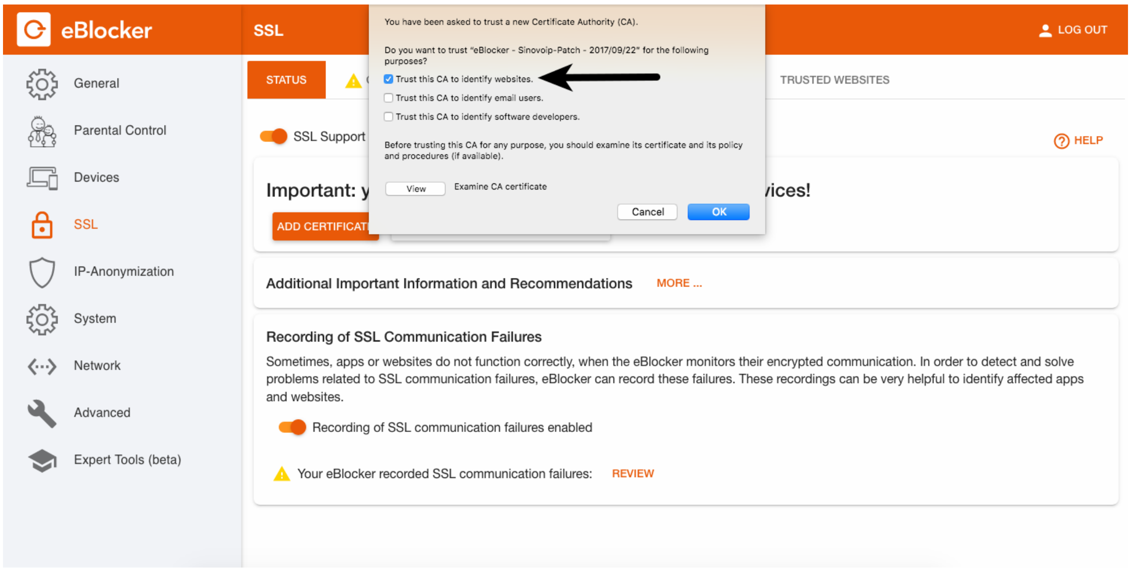
- Firefox
- Cliqz (based on Firefox)
- Seamonkey
- Thunderbird (email program)

Firefox, Cliqz or Seamonkey

Open the eBlocker HTTPS configuration page.

Click on the button add certificate.

Make sure that the first checkbox ,Trust this CA to identify websites' is selected (see image below).



You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "eBlocker - Sinovoip-Patch - 2017/09/22" for the following purposes?

☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

□ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate

Cancel OK

Additional Important Information and Recommendations MORE ...

Recording of SSL Communication Failures

Sometimes, apps or websites do not function correctly, when the eBlocker monitors their encrypted communication. In order to detect and solve problems related to SSL communication failures, eBlocker can record these failures. These recordings can be very helpful to identify affected apps and websites.

Recording of SSL communication failures enabled

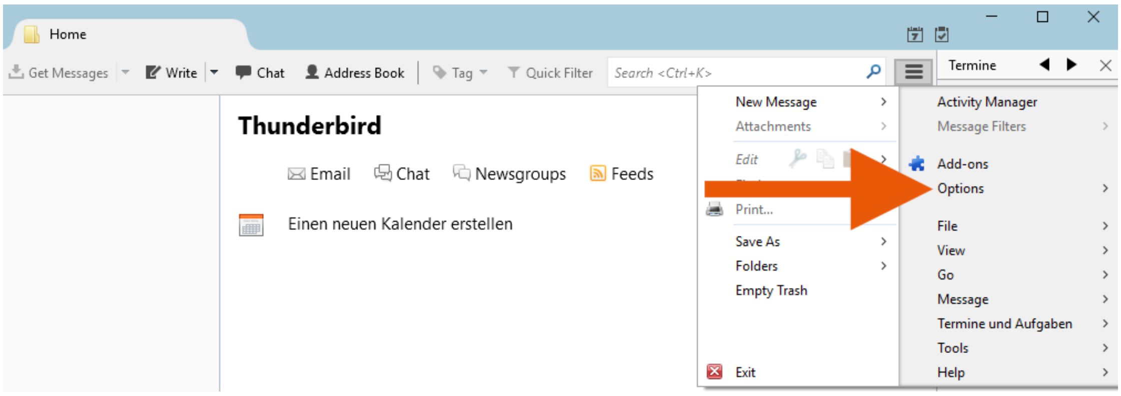
Your eBlocker recorded SSL communication failures: REVIEW

Click on *OK* to insert the eBlocker certificate in Firefox.

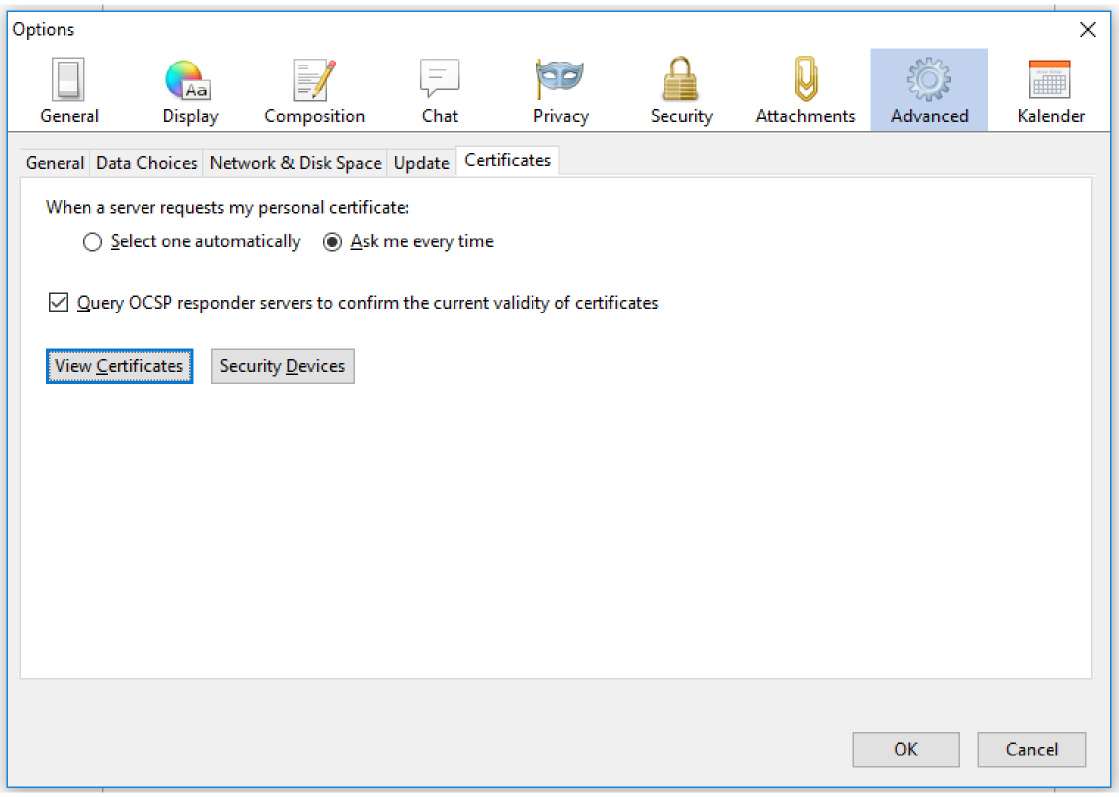
You can see the eBlocker controlbar now on HTTPS sites with the Firefox, Cliqz or Seamonkey browser.

Thunderbird (email program)

Go to the menu and click on *Options*.



Go to *Advanced* and click on *View Certificates*.



Options

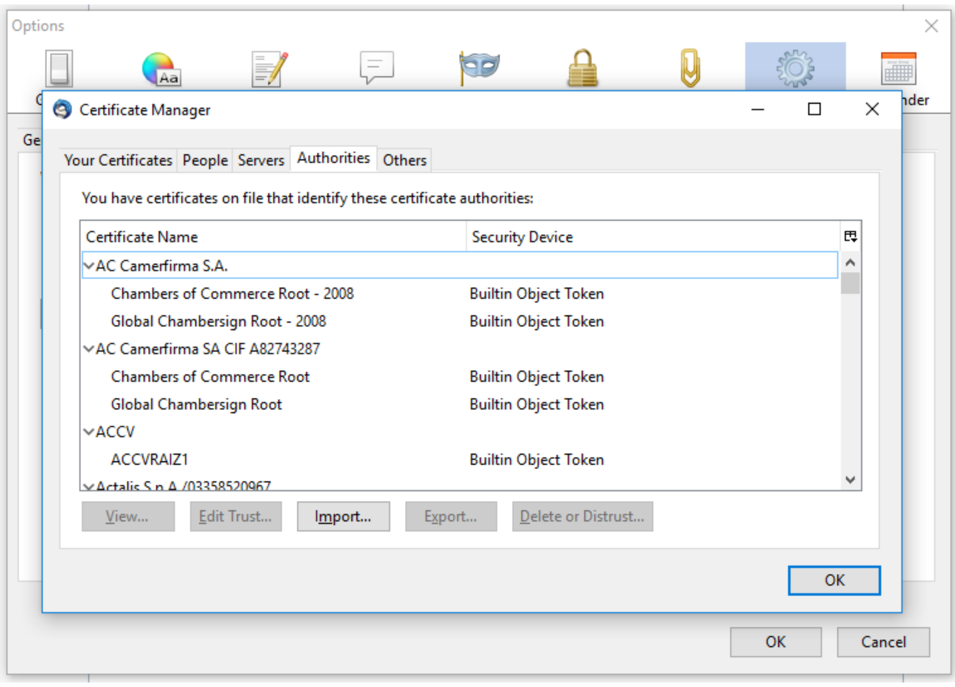
General | Data Choices | Network & Disk Space | Update | Certificates

When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

☑ Query OCSP responder servers to confirm the current validity of certificates

After the Certificate Manager opens, click on *Import* and choose the eBlocker certificate from the downloads directory.

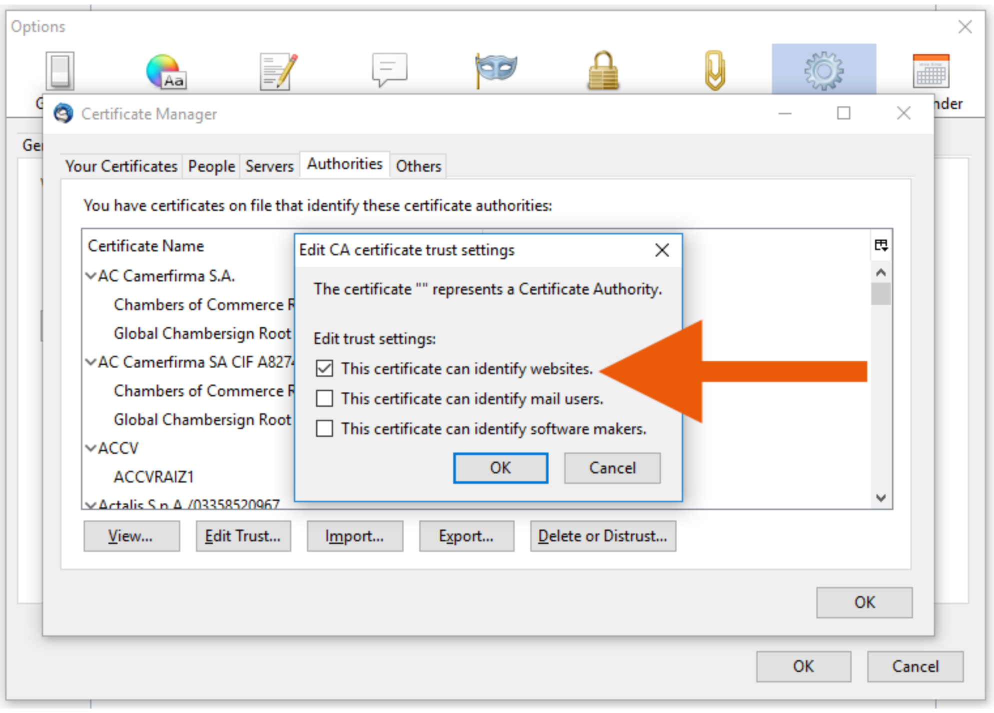


Certificate Manager

You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token
ACCV	
ACCVRAIZ1	Builtin Object Token
Actalis S.p.A./03358520967	

Open the eBlocker certificate and make sure that the first checkbox ‚*This certificate can identify websites*‘ is selected. Confirm with *OK*.



You have certificates on file that identify these certificate authorities:

Certificate Name
AC Camerfirma S.A.
Chambers of Commerce R
Global Chambersign Root
AC Camerfirma SA CIF A827
Chambers of Commerce R
Global Chambersign Root
ACCV
ACCVRAIZ1
Actalis S.p.A./03358520967

Edit CA certificate trust settings

The certificate "" represents a Certificate Authority.

Edit trust settings:

☑ This certificate can identify websites.
□ This certificate can identify mail users.
□ This certificate can identify software makers.

Confirm the Certificate Manager and the settings with *OK*.

The certificate is now inserted into the Thunderbird email program.

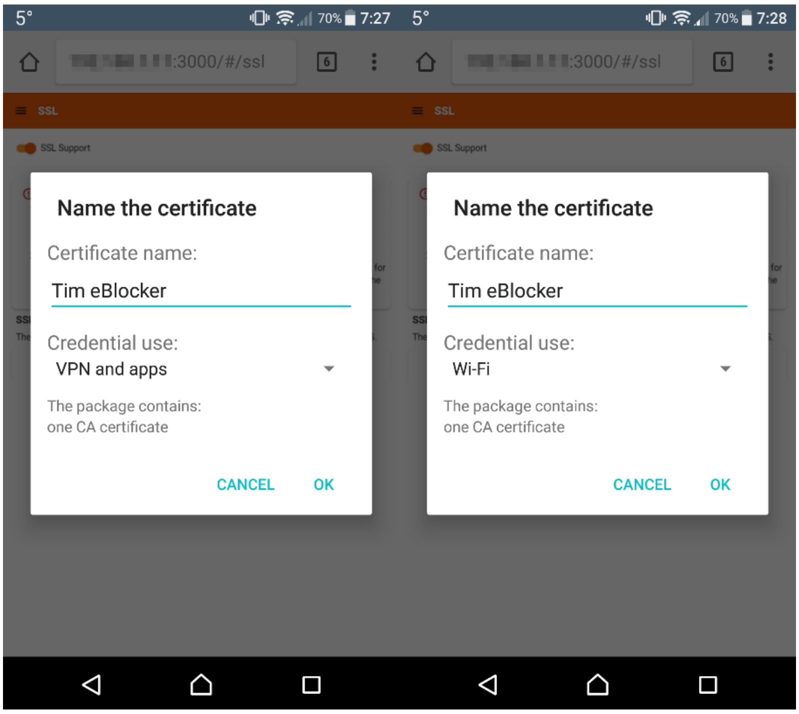
6.2.3 Android

You have added the certificate with only a few clicks. Open the Google Chrome browser.

- Open the eBlocker HTTPS configuration page.
- Click the button "Add certificate".
- Enter your PIN if necessary
- Give the certificate a name (for example: Tim eBlocker).
- Select "VPN and Apps" for credential use.
- Repeat the last steps and save the certificate at "Wi-Fi".

For Android versions smaller than version 6, it is sufficient to save the certificate only at "Wi-Fi".

If the eBlocker certificate is not opened automatically you can find it in your download folder.



5° 70% 7:27

[redacted]:3000/#/ssl

SSL

SSL Support

Name the certificate

Certificate name:

Tim eBlocker

Credential use:

VPN and apps

The package contains:
one CA certificate

CANCEL OK

5° 70% 7:28

[redacted]:3000/#/ssl

SSL

SSL Support

Name the certificate

Certificate name:

Tim eBlocker

Credential use:

Wi-Fi

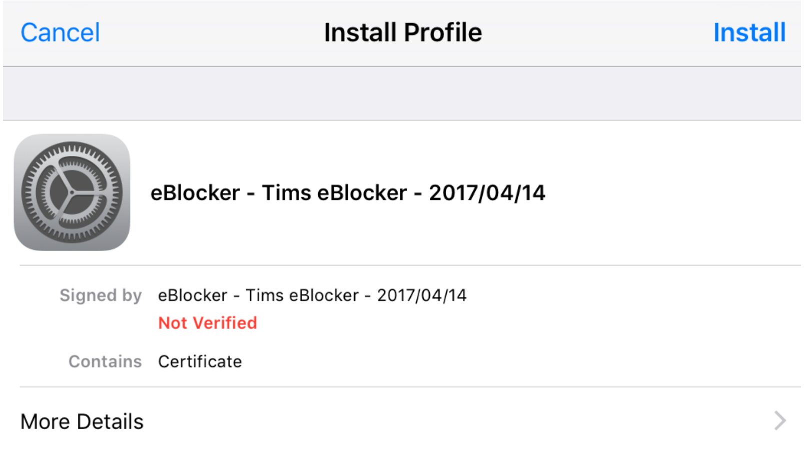
The package contains:
one CA certificate

CANCEL OK

6.2.4 iOS

You have added the certificate with only a few clicks. Open the iOS Safari browser.

- Open the eBlocker HTTPS configuration page..
- Click the button "Add certificate".
- The iOS settings open automatically and the profile of the eBlocker certificate is displayed.
- Click on "Install".
- In the following dialog click on "Install" again.
- Confirm by clicking on "Install" for the last time again.
- The eBlocker certificate has now been added in iOS.



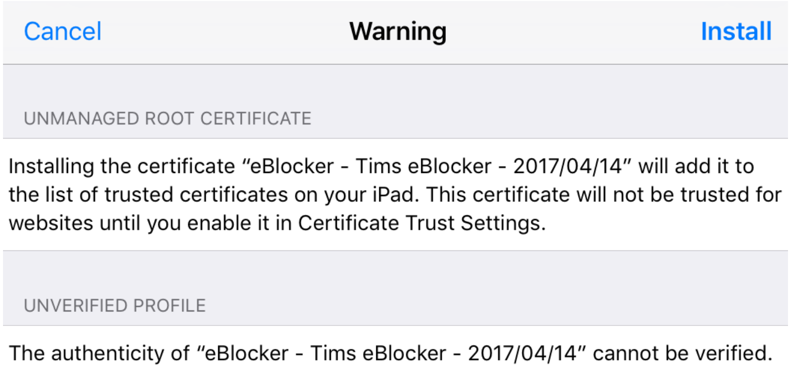
Cancel **Install Profile** Install

eBlocker - Tims eBlocker - 2017/04/14

Signed by eBlocker - Tims eBlocker - 2017/04/14
Not Verified

Contains Certificate

More Details

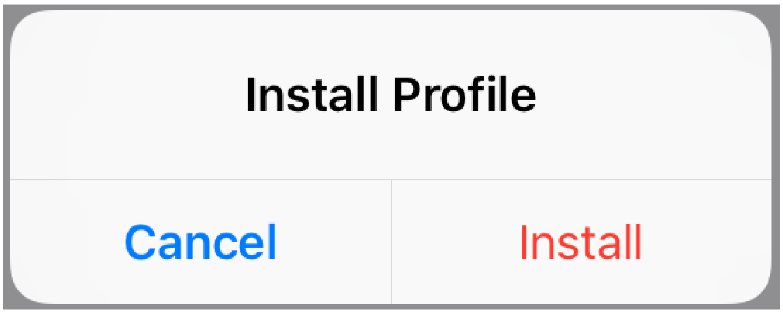


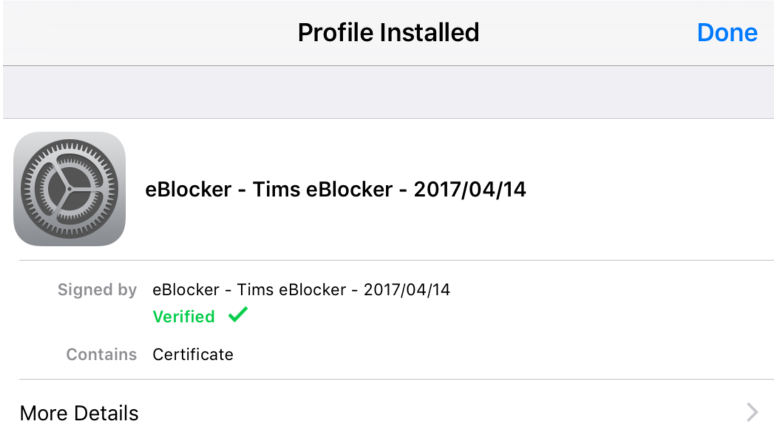
UNMANAGED ROOT CERTIFICATE

Installing the certificate “eBlocker - Tims eBlocker - 2017/04/14” will add it to the list of trusted certificates on your iPad. This certificate will not be trusted for websites until you enable it in Certificate Trust Settings.

UNVERIFIED PROFILE

The authenticity of “eBlocker - Tims eBlocker - 2017/04/14” cannot be verified.





eBlocker - Tims eBlocker - 2017/04/14

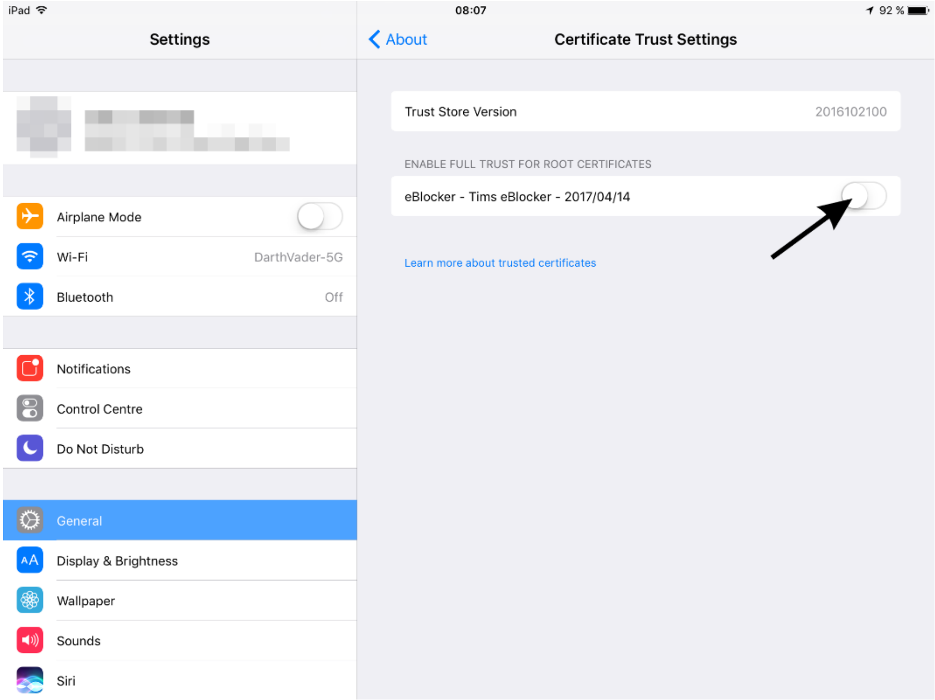
Signed by eBlocker - Tims eBlocker - 2017/04/14
Verified ✓

Contains Certificate

More Details >

Starting with the iOS version 10.3 the added eBlocker certificate has to be activated again.

- Open iOS Settings and navigate to "General" > "About" > "Certificate Trust Settings".
- There you will find the previously added eBlocker certificate that you can now activate.



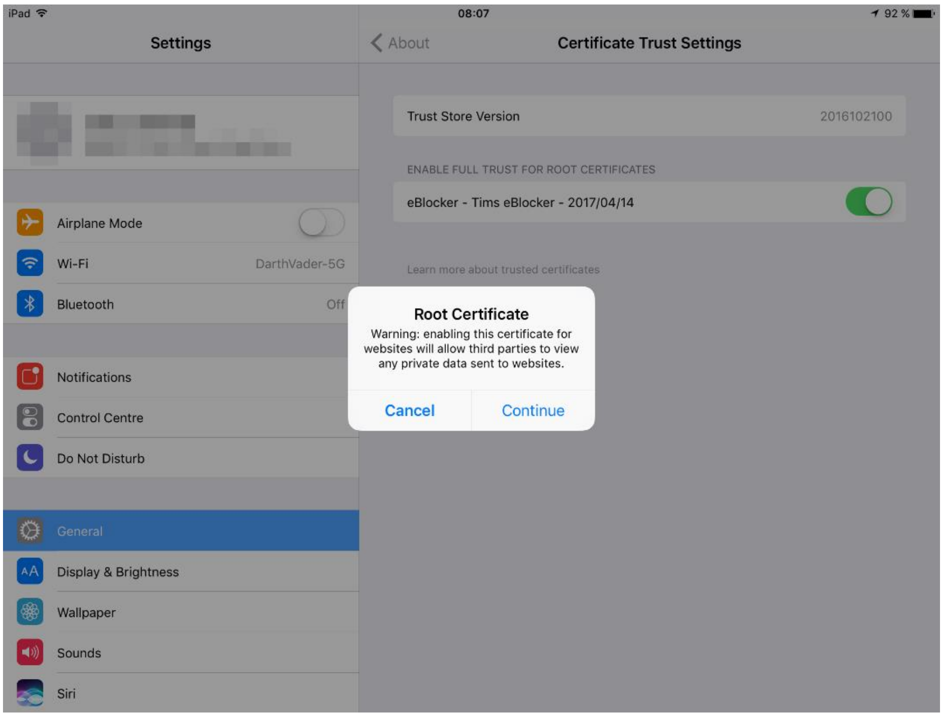
Certificate Trust Settings

Trust Store Version 2016102100

ENABLE FULL TRUST FOR ROOT CERTIFICATES

eBlocker - Tims eBlocker - 2017/04/14

Learn more about trusted certificates



Certificate Trust Settings

Trust Store Version 2016102100

ENABLE FULL TRUST FOR ROOT CERTIFICATES

eBlocker - Tims eBlocker - 2017/04/14

Learn more about trusted certificates

Root Certificate

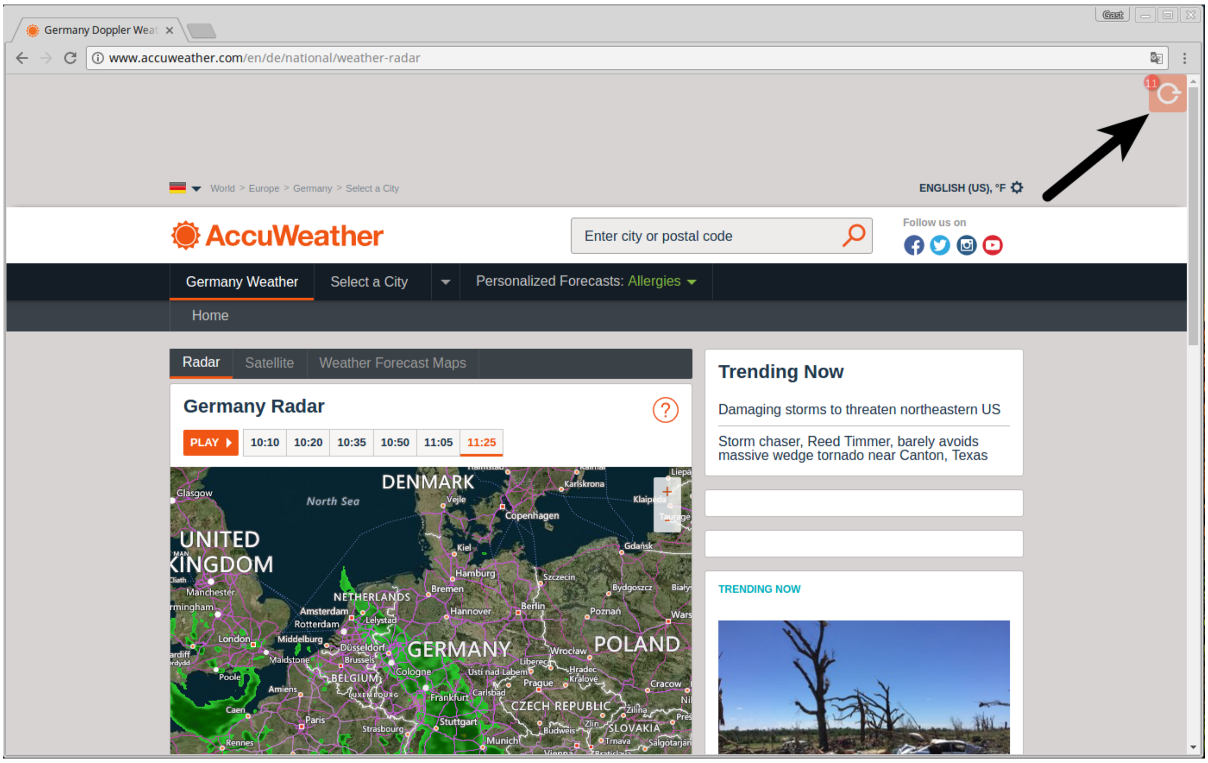
Warning: enabling this certificate for websites will allow third parties to view any private data sent to websites.

7 Definition of eBlocker functions

At daily use, you usually shouldn’t notice your eBlocker right away. Everything should work fine. A lot of sites will even load faster because advertisements and animations are blocked.

7.1 eBlocker icon

You can see if the eBlocker is working and activated by the orange translucent icon that is visible on the top right of every browser that you use.


Germany Doppler Wea
www.accuweather.com/en/de/national/weather-radar
11
World > Europe > Germany > Select a City
ENGLISH (US), °F
AccuWeather
Enter city or postal code
Follow us on
Germany Weather
Select a City
Personalized Forecasts: Allergies
Home
Radar
Satellite
Weather Forecast Maps
Germany Radar
PLAY
10:10
10:20
10:35
10:50
11:05
11:25
Trending Now
Damaging storms to threaten northeastern US
Storm chaser, Reed Timmer, barely avoids massive wedge tornado near Canton, Texas
TRENDING NOW
DENMARK
UNITED KINGDOM
GERMANY
POLAND

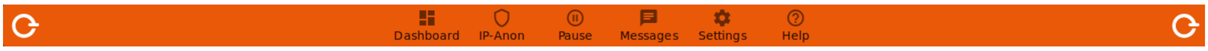
If trackers or advertisements are blocked on the site, the total number of blocked requests will be displayed. Through a click on the eBlocker icon you can have access to the controlbar.

7.2 eBlocker Controlbar Base, Pro, Family

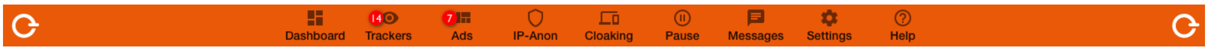
Through the controlbar you have quick access to the most important features for the currently loaded page or for the device you are currently using.

The features of the eBlocker Controlbar differ depending on the eBlocker version.

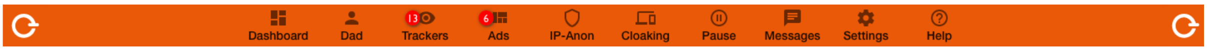
eBlocker Base



eBlocker Pro



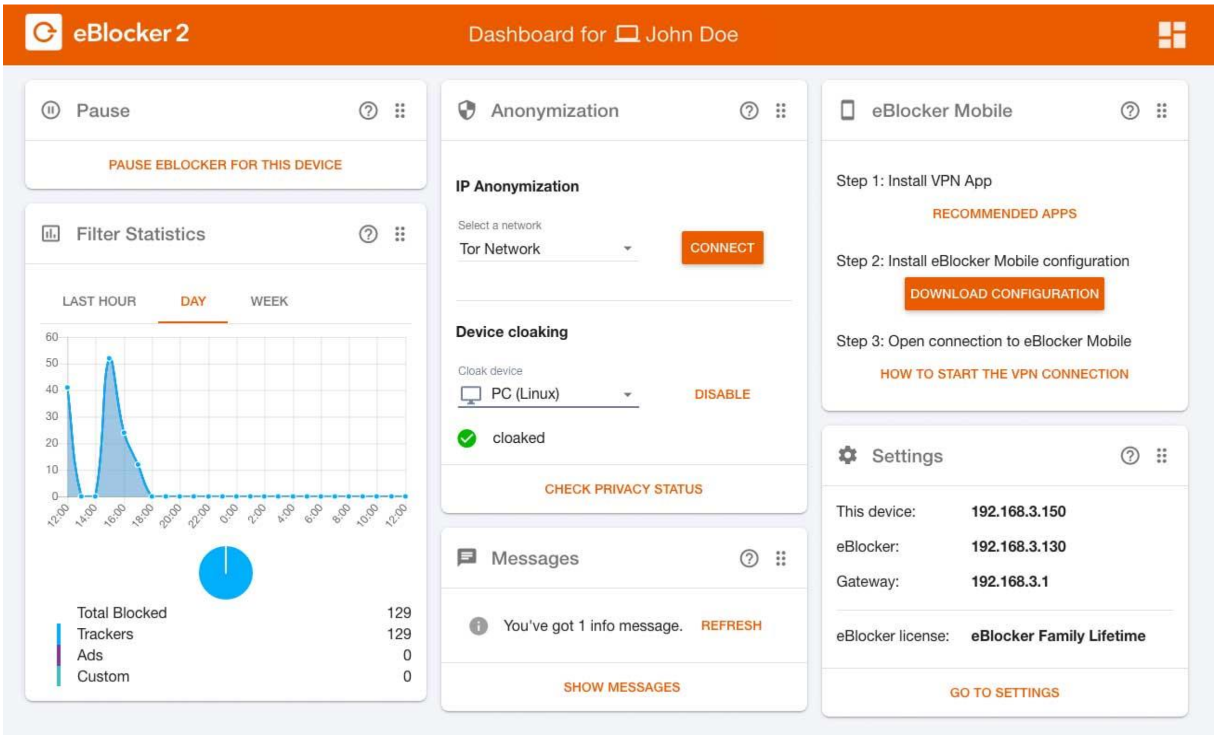
eBlocker Family



You can read detailed information about the functions in the following sections.

7.3 Dashboard

With a click on "Dashboard" you open the Dashbard of the eBlocker in a new browser tab. The Dashboard offers you the same range of features as the eBlocker Controlbar. It also provides quick access to the settings of your eBlocker.



Total Blocked	129
Trackers	129
Ads	0
Custom	0

IP Anonymization

Select a network: Tor Network

Device cloaking

Cloak device: PC (Linux)

cloaked

You've got 1 info message.

Step 1: Install VPN App

Step 2: Install eBlocker Mobile configuration

Step 3: Open connection to eBlocker Mobile

This device:	192.168.3.150
eBlocker:	192.168.3.130
Gateway:	192.168.3.1
eBlocker license:	eBlocker Family Lifetime

Tip: Bookmark the eBlocker Dashbard in your browser, or use the eBlocker Dashboard as your home page. For more information on the eBlocker Dashboard, read our article "Tips on the eBlocker Dashboard" in our forum/ knowledge base.

Following menus in the dashboard you can arrange with the mouse as you like:

Pause
Here you can pause your eBlocker for this device. The pause is started for 5 minutes, but can be extended or shortened for another 5 minutes at any time.

Setting
Here you can see the IP addresses of your device, your eBlocker and your gateway (router). Additionally you can see your eBlocker license and can open the eBlocker settings.

Messages
In certain cases, your eBlocker can send you messages. You can display these here.

Conrolbar
Here you can determine if and where (left and right) the eBlocker icon should be displayed in the browser. For example, you can display the eBlocker icon for only 5 seconds. The settings "Only in standard browsers" should prevent you from seeing the eBlocker icon in apps if necessary.

HTTPS-Support (only for eBlocker Pro and eBlocker Family)
Here you can activate HTTPS support for your device and also download the eBlocker certificate. In addition, this menu also checks whether the eBlocker certificate has been stored correctly.

Anonymization (only for eBlocker Pro and eBlocker Family)
Here you can choose whether you want to surf via Tor or a VPN connection.
If the HTTPS feature of the eBlocker is activated, you can also activate the device cloaking in this menu. Additionally you have the possibility to test your privacy status here. For this purpose we have created a special website for you.

Blocker Statistics (only for eBlocker Pro and eBlocker Family)
Here you can see the statistics of the blocked contents for the last hour, the last day, or the last week.

Blocker Statistics (overview) (only for eBlocker Pro and eBlocker Family)
Here you can see a more detailed statistic of the blocked content since the last start of the eBlocker. The top 25 domains for the trackers and advertising are displayed separately.

Tracker and Ad Blocking Rules (only for eBlocker Pro and eBlocker Family)
Here you can specify whether the eBlocker should block all connections to trackers or to advertisements. If these two settings are deactivated, your eBlocker will also not block trackers and advertisements. You can also allow certain connections to a domain in a whitelist for this device, or block additional domains for a device in a blacklist.

eBlocker Mobile
Here you can download the OpenVPN configuration for the eBlocker Mobile feature for your device. If the eBlocker Mobile feature is not activated, you will not be able to see this menu.

User (only for eBlocker Family)
If your device is assigned to a user, this menu can be displayed.
Here you can, for example, take over a user's device, change the PIN for this device, or lock the device.

7.4 Tracker and Ads (Tracker- and Ad-Blocker)

Available for **eBlocker Pro** and **eBlocker Family**

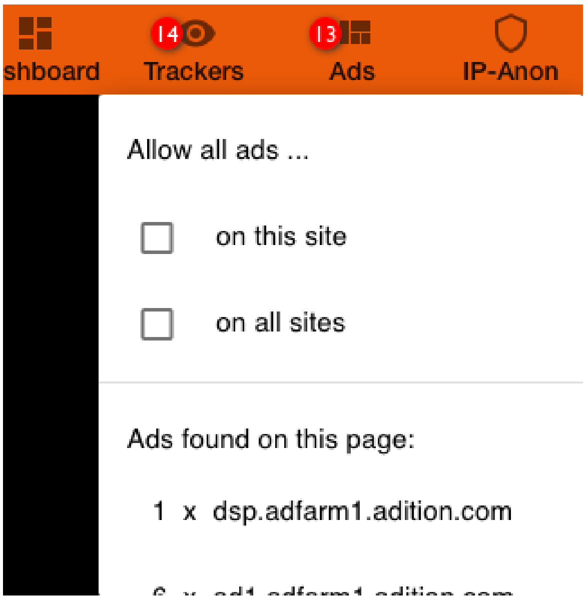
One of the main and most important functions of the eBlocker is to prevent third parties from analyzing your surfing behavior and thus creating a detailed personality profile of you.

The eBlocker blocks the transmission of data to data collectors by default and prevents the loading of advertisements from advertising networks, that also log your surfing behavior and compress it to profiles.

The controlbar lets you can see how many connections to data collectors and advertising networks have been prevented on each page. By clicking on the "Tracker" and "Ads" icons, you can see how many trackers and ads have been blocked in the last 60 seconds and 10 minutes. You will also see a list of all blocked connections.

eBlocker wants to protect your privacy but the eBlocker does not try to avoid possible content blockings of the publishers. Websites such as bild. de for e.g., recognize that the eBlocker also blocks advertising and may no longer provide the requested content available for free.

By clicking on "Ads" on the controlbar, you can disable the eBlocker module to filter advertising either globally, or individually for this website and then have access to the content. You can reactivate filtering just as easy. The tracker blocker is still active, so you will continue to be protected from trackers. Be careful: even if the tracker blocker is active, advertising will capture your personality profile.



Allow all ads ...

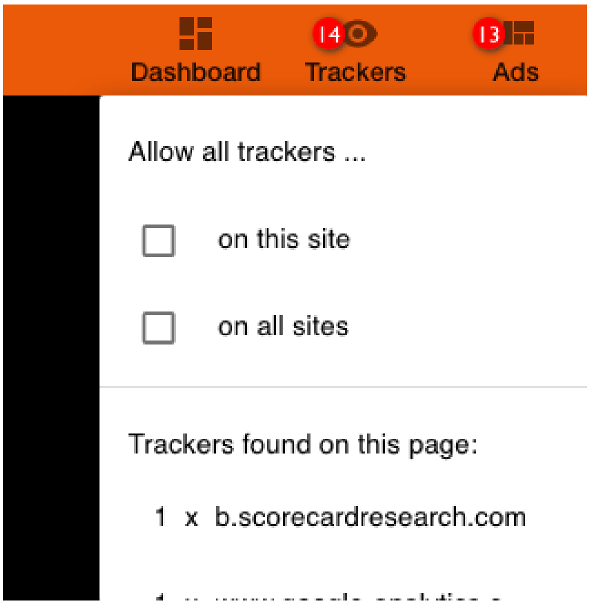
□ on this site

□ on all sites

Ads found on this page:

1 x dsp.adfarm1.adition.com

Just like the module for filtering advertisements, the module for filtering trackers can be deactivated or activated globally, or individually for a website.



Allow all trackers ...

□ on this site

□ on all sites

Trackers found on this page:

1 x b.scorecardresearch.com

Websites for which you allow ads or trackers, will be listed on the eBlocker Dashboard. There you can either allow or disable the ads and trackers for the desired page as well.

7.5 Anon (IP-Anonymization)

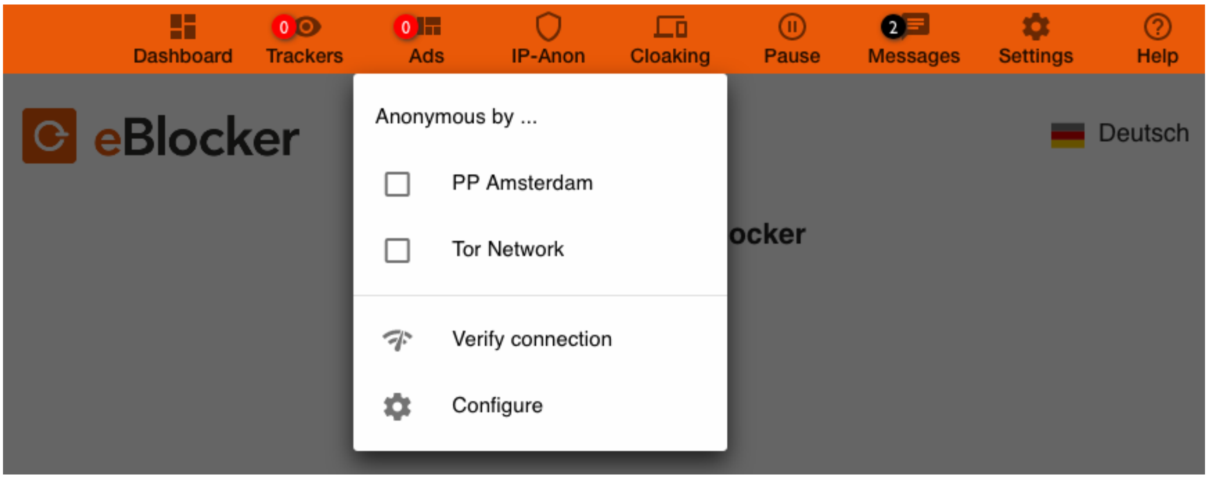
Whenever you are on the Internet, you transmit your so-called IP address to the website you are visiting. It's kind of like the number transmission on the phone. There is no public "phonebook" for IP addresses, but your Internet provider knows who used which IP address and when. These data - keyword "data retention" - are also stored for a period of time and, if necessary, passed on to the state authorities.

Regardless of this, each IP address can always be assigned to the provider and also to a geographical region.

To disguise your own IP address, i. e. to achieve additional anonymity on the Internet, you can activate the “IP Anonymization”.

Once “IP Anonymization” is switched on, all HTTP requests are routed through an anonymization network. If SSL/HTTPS is activated on the eBlocker, HTTPS requests will also be anonymized. We are now able to support alternative networks with the OpenVPN protocol.

For information on how to set up and use the Tor network, see chapter 8.5.
For information on how to set up and use other networks, see chapter 8.5.2



With "Check connection" you can check whether a connection via a Tor anonymizing network exists or which external data is visible.

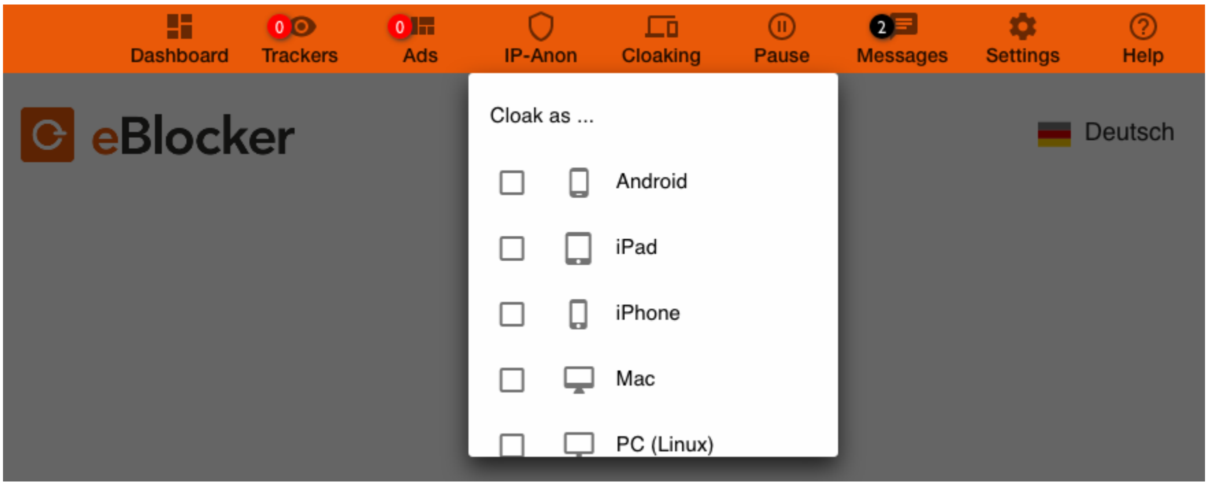
With "Configure" you can directly go to the settings "IP Anonymization".

7.6 Cloaking

Available for **eBlocker Pro** and **eBlocker Family**

Each internet browser identifies itself with the so-called "User Agent" -identification. This identifier provides the website with precise information on the end device, operating system and browser used. It is not only used to identify you and to create a personality profile but it is also used by shops very often to offer individual prices. For e.g., if you use a tablet you will may get a different price for the same product as you would by using a stationary PC.

You can use the “Device Cloaking” feature of the eBlocker to cloak your device and cause the user agent ID of another device type to be sent. This allows you to further improve the protection of your privacy and ideally to take advantage from dynamic pricing in some shops.



Cloak as ...

- ☐ Android
- ☐ iPad
- ☐ iPhone
- ☐ Mac
- ☐ PC (Linux)

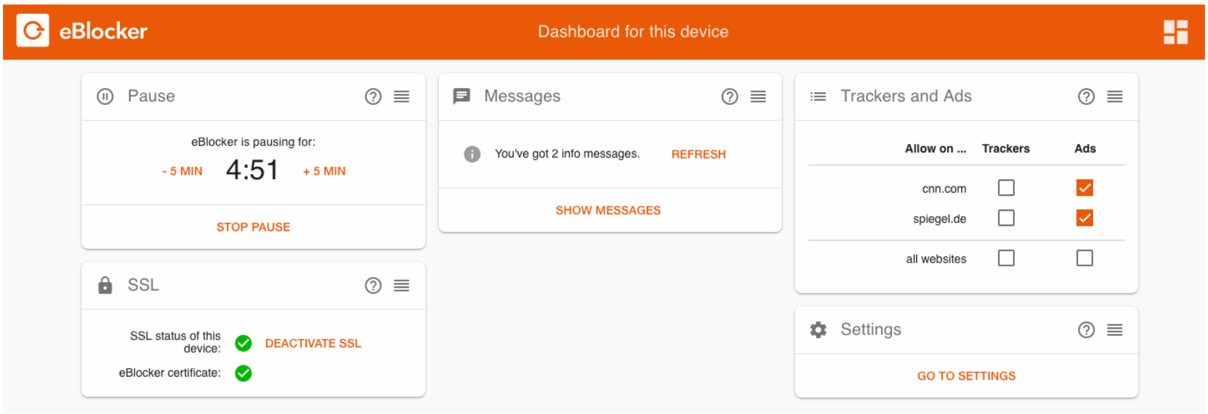
Open the controlbar. Go to "Cloaking" and cloak your device with a click on the device you want be cloaked.

7.7 Pause

Available for **eBlocker Base**, **eBlocker Pro** and **eBlocker Family**

"Pause" deactivates the eBlocker for the current device you are currently surfing with on the Internet.

The eBlocker Dashboard opens in a new browser tab as soon as you click on "Pause" in the eBlocker Controlbar. You can extend the pause in the Dashboard by 5 minutes, shorten, end the pause, or access the eBlocker settings.



eBlocker is pausing for: 4:51

You've got 2 info messages.

Allow on ...	Trackers	Ads
cnn.com	☐	☑
spiegel.de	☐	☑
all websites	☐	☐

SSL status of this device: ✓

eBlocker certificate: ✓

7.8 Settings

Click on „Settings“ to set up your eBlocker individually. Detailed information about the eBlocker functions are described in section 8.

7.9 Help

For questions and issues you can have access to this user manual. Moreover you can go to our forum for technical matters, in which you can find many answers to common asked questions.

http://forum.eBlocker.com

We are also pleased to help you with further assistance via email (see Appendix D).

Unfortunately we do not offer any support via telephone at the moment.

8 The eBlocker settings

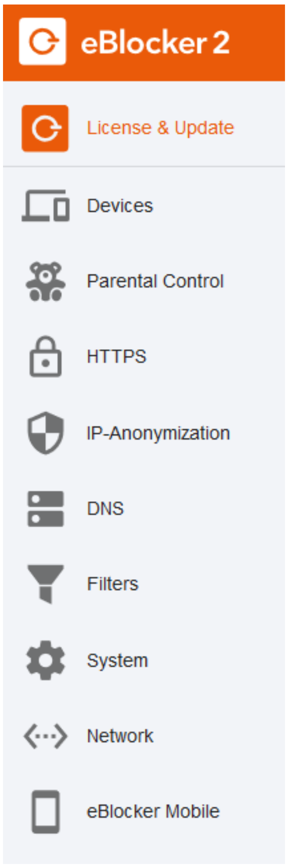
You can find the main functions that you need for your daily routine in the net by clicking on the eBlocker icon (at the right top of every browser site) and through your controlbar (see 7).

Some settings can be adjusted easier and sometimes only through the so called console. You can have access to the setting console by clicking on the icon “Settings” after opening the controlbar (see **Fehler! Verweisquelle konnte nicht gefunden werden.**).

The features of the setting console are divided into following sections:

Section:	**Available for:**
License & Update	eBlocker Base, eBlocker Pro und eBlocker Family
Devices	eBlocker Base, eBlocker Pro und eBlocker Family
HTTPS	eBlocker Pro und eBlocker Family
IP Anonymization	eBlocker Base, eBlocker Pro und eBlocker Family
DNS	eBlocker Base, eBlocker Pro und eBlocker Family
Blocker	eBlocker Pro und eBlocker Family
Network	eBlocker Base, eBlocker Pro und eBlocker Family
eBlocker Mobile	eBlocker Base, eBlocker Pro und eBlocker Family

You can have access to the requested area by clicking on one of the captions listed on the side register, which you see on the left side.



You can find a detailed description for all areas in the following sections.

If you have called the setting console for the first time or if you have not activated the update license yet, the network setting assistant will appear by default. The network setting assistant will guide you through the activation process.

8.1 General

General settings and information about your eBlocker.

This site is divided into following sections:

8.1.1 License

You can read details about your activation status of your license and of your eBlocker here.

By clicking on „Activate new license“ you can update your license (e.g. to lifetime license) or upgrade your license (e.g. from eBlocker Pro to eBlocker Family). Please enter your license key for that.

The link „Buy license“ leads you to our eBlocker online shop.

The link „Transfer license (from/to other device) leads you to a website where you can remove the license off your device and use it for a different device.

8.1.2 Updates

This page shows you which versions of the eBlocker software and filter rules are currently in operation.

You can enable automatic updates, if you have activated a valid license for this device. You can also determine at what time these updates should be implemented.

Automatic updates are activated by default in the general settings and are implemented in your local time between 02:00 o’clock and 03:00 o‘clock.

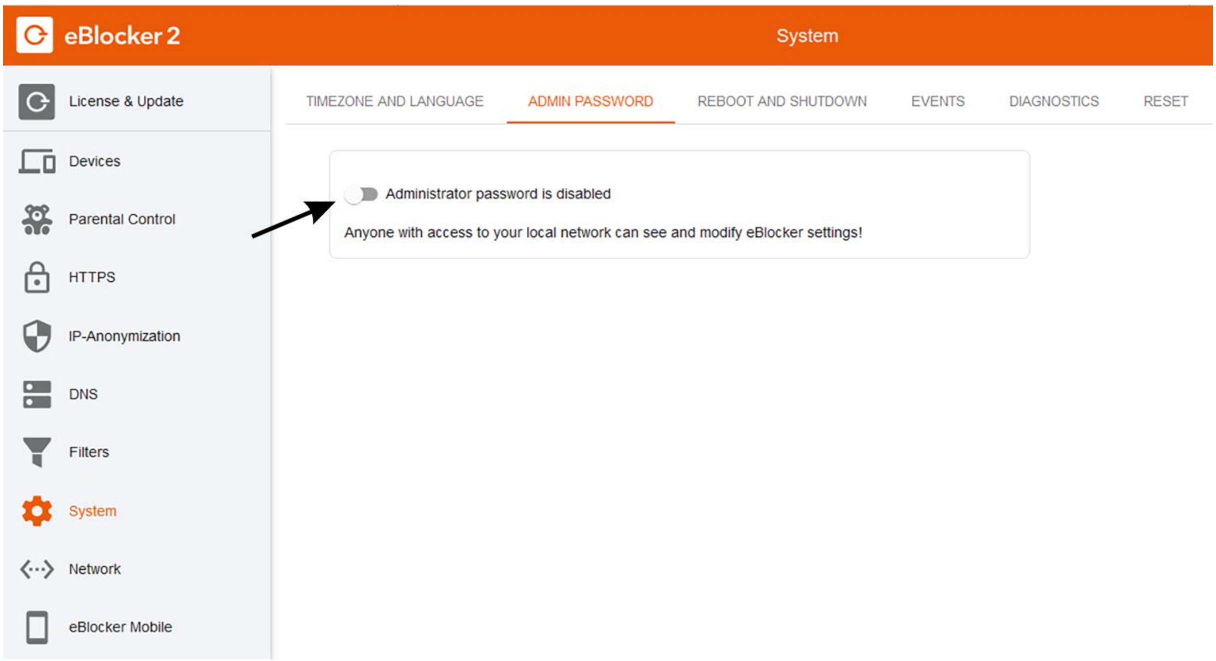
If you deactivate the automatic updates, you can always import updates by yourself. The eBlocker will display a notice next to the "Check for update" button, as soon as a new update is available for you.

8.1.3 Admin-Password

The eBlocker console can be reached through the general settings in your local network, by default. In many cases this is sufficient and very practical.

However, we recommend to assign an administrator password, so that important settings and information of your eBlocker are only accessible after entering this password. Once a password has been assigned, your eBlocker console can only be accessed by entering this password.

Please keep the admin-password in safe hands! In case you forget your password or mislay it, you can reset the password by clicking on the slide switch near the words “Administrator password is disabled”.



Administrator password is disabled

Anyone with access to your local network can see and modify eBlocker settings!

You can find some general and legal basics as well as references to your eBlocker. You can also read about how to get in touch with our support forum (see Appendix D).

8.2 Parental Control

If you have used Parental Control already in a previous version, please consider the hints in section 8.2.19

8.2.1 Activate Parental Control

To be able to use Parental Control, assign an administrator password first to prevent others from accessing the eBlocker settings and perhaps deactivating Parental Control.

Assign the administrator password in the "eBlocker Settings > System" at "Admin Password".

Navigate to "eBlocker Settings > Parental Control". The section “Parental Control” is divided into four subpages. We describe the functions detailed in the following sections:

- User
- User Profile
- Website Blacklists
- Website Whitelists

8.2.2 User and Protection profiles

In order to activate Parental Control for individual devices in your home network, all devices that should be protected must first be assigned to a user. This user will define the effective protection profile for the device. The protection profile then defined the access rules for the device. I.e. it defines, which websites are accessible or restricted and at which times and how long internet access is permitted.

New in release 1.3: The active user of a device - and thus the active protection profile - can now be changed at any time by entering a user PIN, so that a flexible use of the devices is possible.

Example 1:
The family tablet is accessible to every family member, even children can use it at any time without the parent having to attend. Therefore, the tablet should be assigned to a user with a restricted protection profile to ensure maximum protection during unattended use. If a parent wants to use the tablet, the Parental Control protection can temporarily be changed or switched off by changing the user of the device. A PIN must be entered for the user change. Once the parent has finished using the device, the user should be reset to the original owne, or the Internet access for the device should be completely blocked.

Example 2:
A parent's smartphone is always owned by that parent. It is also protected against unauthorized use by a system password. The children can never use this smartphone unattended. In this case, it is not necessary to assign an explicit user or a Protection profile to the device.

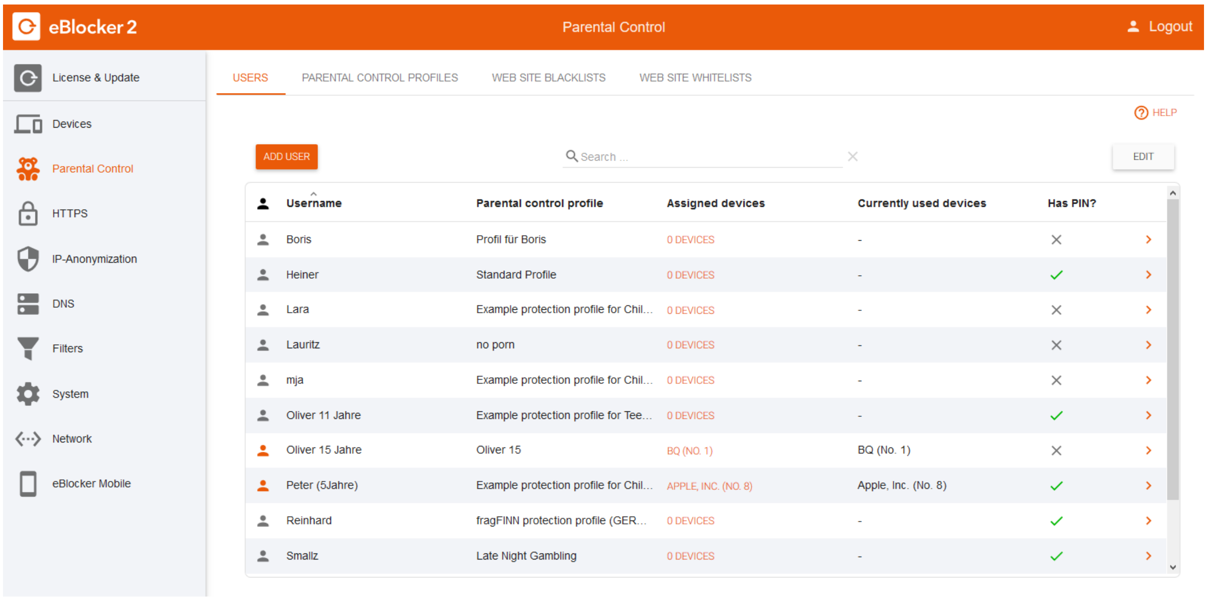
8.2.3 Three easy steps

The following steps must be carried out to activate Parental Control for your home network:

- Create an eBlocker user for all family members (see section 8.2.4).
- Assign the appropriate protection profile to each user. The eBlocker provides sample profiles that can be adapted to your needs. Or you can set up additonal protection profiles yourself (see section 8.2.7).
- Assign a main user to all devices that should be protected by Parental Control (see section 8.2.11). It is possible to change the active user of a device at any time by entering an individual user PIN (see section 8.2.18).

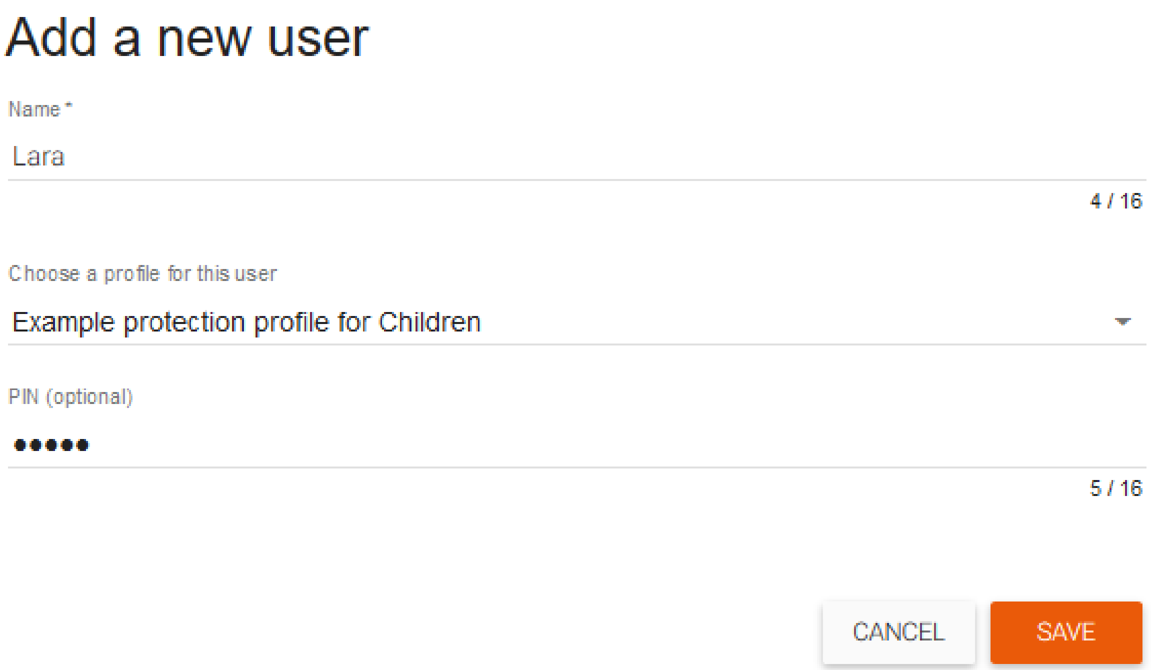
8.2.4 Create a new user

Navigate to the “eBlocker Settings > Parental Control” and click on the page “User”. If you have not used Parental Control yet, the list of users is empty. After you have created some users, the page might look like this:



Username	Parental control profile	Assigned devices	Currently used devices	Has PIN?
Boris	Profil für Boris	0 DEVICES	-	✗
Heiner	Standard Profile	0 DEVICES	-	✓
Lara	Example protection profile for Chil...	0 DEVICES	-	✗
Lauritz	no porn	0 DEVICES	-	✗
mja	Example protection profile for Chil...	0 DEVICES	-	✗
Oliver 11 Jahre	Example protection profile for Tee...	0 DEVICES	-	✓
Oliver 15 Jahre	Oliver 15	BQ (NO. 1)	BQ (No. 1)	✗
Peter (5Jahre)	Example protection profile for Chil...	APPLE, INC. (NO. 8)	Apple, Inc. (No. 8)	✓
Reinhard	fragFINN protection profile (GER...	0 DEVICES	-	✓
Smallz	Late Night Gambling	0 DEVICES	-	✓

To create a new user, click “Add User”. A dialog box (see below) opens. Enter a name and select a Protection profile. In addition, you should assign a PIN to all users who are allowed to use another device. For example, provide a PIN for all adults and the older children.



Add a new user

Name *

Lara

4 / 16

Choose a profile for this user

Example protection profile for Children

PIN (optional)

●●●●●

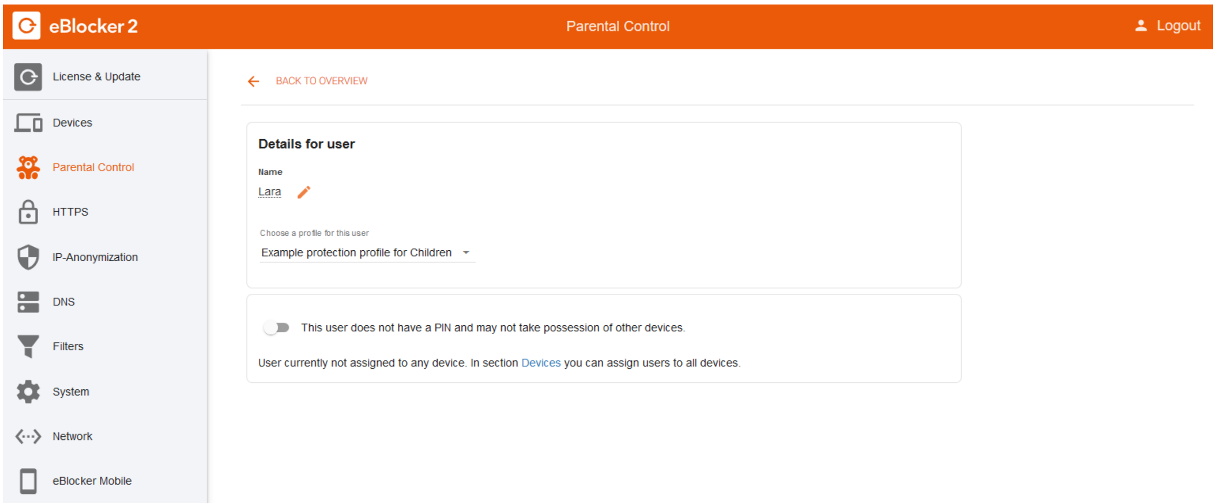
5 / 16

Note that any user who has received a PIN can change their own PIN over the ControlBar (s. section 8.2.18). You can also view and change all other settings at any time.

8.2.5 Change settings of a user

Click on the name of a user. The current settings and details for this user will be displayed:

eBlocker
Switch on Privacy.



Details for user

Name
Lara

Choose a profile for this user
Example protection profile for Children

This user does not have a PIN and may not take possession of other devices.

User currently not assigned to any device. In section Devices you can assign users to all devices.

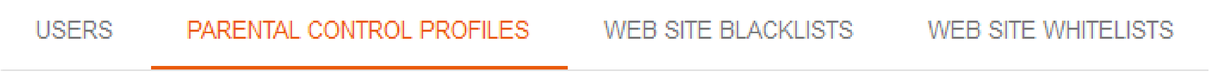
You can change the name of the user, select another protection profile for the user, and specify whether the user is allowed to accept other devices by entering a PIN or not.
In addition, you can see which devices this user is assigned to as main user, and whether the user is currently active on other devices.

8.2.6 Remove User

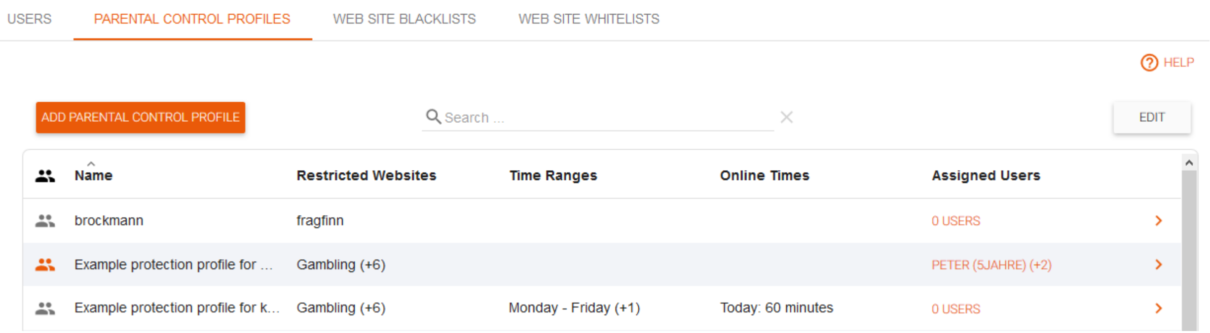
You can remove a user with the button "Remove user" in the detailed view of the user (see above). However, the button is disabled when devices are still assigned to the user. First assign a different user to the corresponding devices to activate the button.

8.2.7 Create new profile

Navigate to the “eBlocker Settings > Parental Control” and click on the page “User Profiles”.



The eBlocker provides a default “Standard Profile” as well as a few sample profiles with Parental Control restrictions:

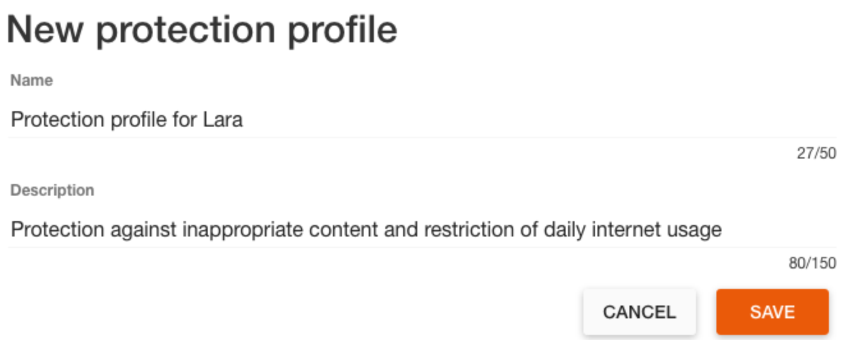


Name	Restricted Websites	Time Ranges	Online Times	Assigned Users
brockmann	fragfinn			0 USERS
Example protection profile for ...	Gambling (+6)			PETER (5JAHRE) (+2)
Example protection profile for k...	Gambling (+6)	Monday - Friday (+1)	Today: 60 minutes	0 USERS

The Standared Profile does not contain any restrictions on Internet access. It is automatically assigned to all existing and new devices in the home network.

In addition, the eBlocker provides predefined Protection profiles for different requirements as examples and suggestion.

Click on the button "New Protection Profile" to create a new Protection profile. In order to keep your profiles apart, assign names and a brief description. Save the profile afterwards.



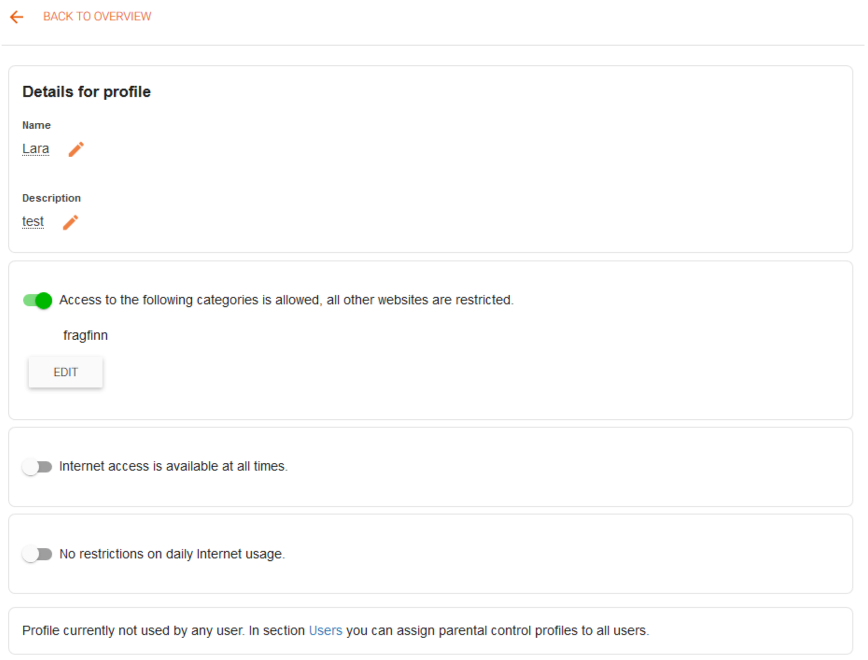
New protection profile

Name: Protection profile for Lara
27/50

Description: Protection against inappropriate content and restriction of daily internet usage
80/150

To access the settings of the profile you just created, click on it in the list.
You can change the name and description of the profile, modify site and category filters, create time constraints, or delete the profile.

In the profile details, you can also see to which users the profile is currently assigned.
Initially, no Parental Control restrictions are activated in a new profile and no users are assigned to it:



Details for profile

Name: Lara

Description: test

Access to the following categories is allowed, all other websites are restricted.

fragfinn

Internet access is available at all times.

No restrictions on daily Internet usage.

Profile currently not used by any user. In section Users you can assign parental control profiles to all users.

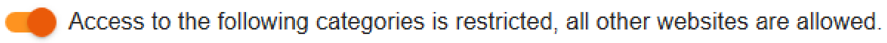
You can now adjust the following settings to create a Protection profile according to your needs:

- Deny or allow access to certain categories of websites.
- Allow Internet access only at certain times of the day.
- Limit the maximum Internet usage time per day.

Details to all settings can be found in the next sections.

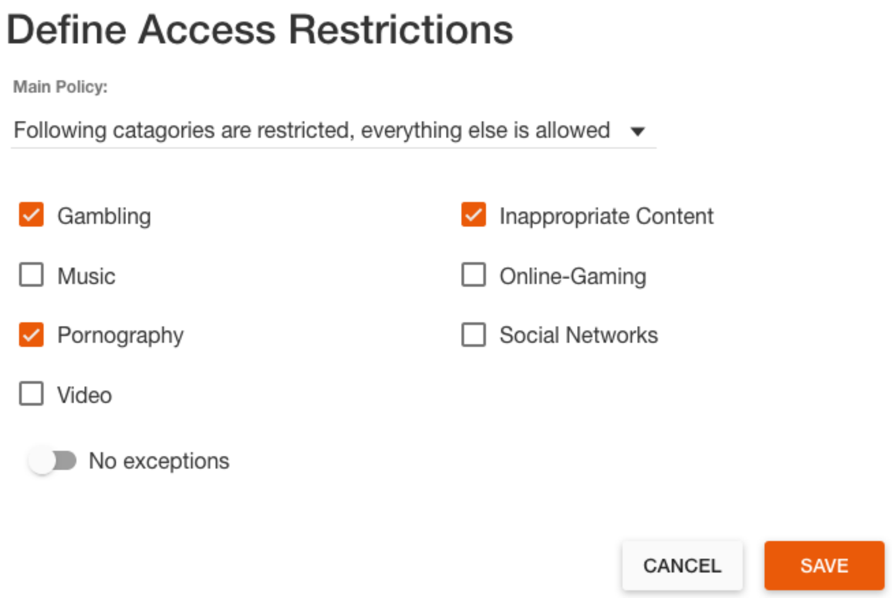
8.2.8 Deny access to categories of websites

To deny access to certain categories of sites, activate the site category filter by clicking the slider button.



Access to the following categories is restricted, all other websites are allowed.

The following Dialog box opens:



Define Access Restrictions

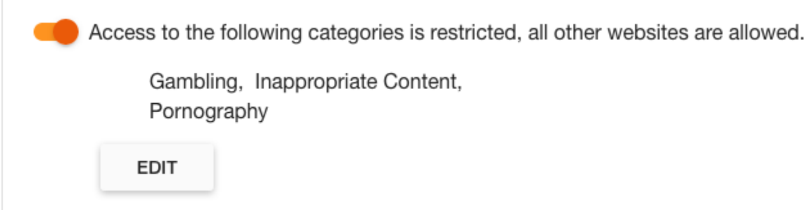
Main Policy:
Following catagories are restricted, everything else is allowed ▾

☑ Gambling ☑ Inappropriate Content
□ Music □ Online-Gaming
☑ Pornography □ Social Networks
□ Video

No exceptions

When you move the mouse over the list of categories, you will be informed of the content of the categories by a tooltip. Select the categories that should be banned for the profile and save the settings.

The filters are then generated for this profile. This may take a few seconds because some lists have literally millions of entries. You can adjust the website category filter at any time by clicking on the "Edit" button:



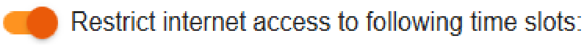
Access to the following categories is restricted, all other websites are allowed.

Gambling, Inappropriate Content,
Pornography

Further details on the category filters and how you can create your own categories of blacklisted or whitelisted websites can be found in sections 8.2.15 and 8.2.17. The eBlocker provided category filters are automatically updated daily. To disable the restrictions of the category filter completely, deactivate the corresponding sliding switch.

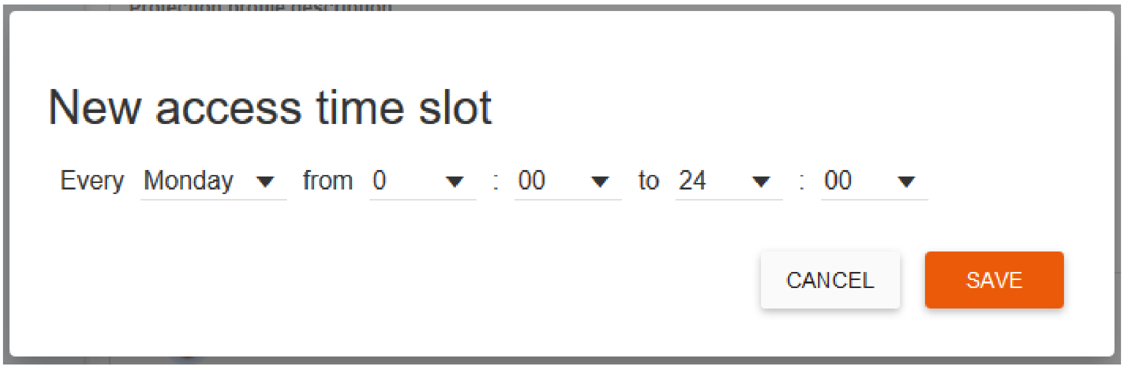
8.2.9 Restrict internet access to certain time slots a day

For each day of the week, you can specify one or more time slots that allow access to the Internet through this profile. Activate the sliding switch to restrict the internet access:



Restrict internet access to following time slots:

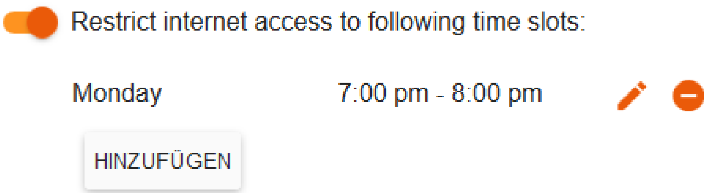
If no time periods have yet been defined, the following dialog box opens directly:



New access time slot

Every Monday from 0 : 00 to 24 : 00

After adding the first time slot, the configuration is displayed like this:



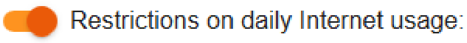
Restrict internet access to following time slots:

Monday 7:00 pm - 8:00 pm

To add more time slots, click the "Add" button. To change predefined slots, click the pencil icon next to the slot. To remove slots again, click the minus symbol next to the slot. To completely disable the restriction on time slots, deactivate the corresponding sliding switch.

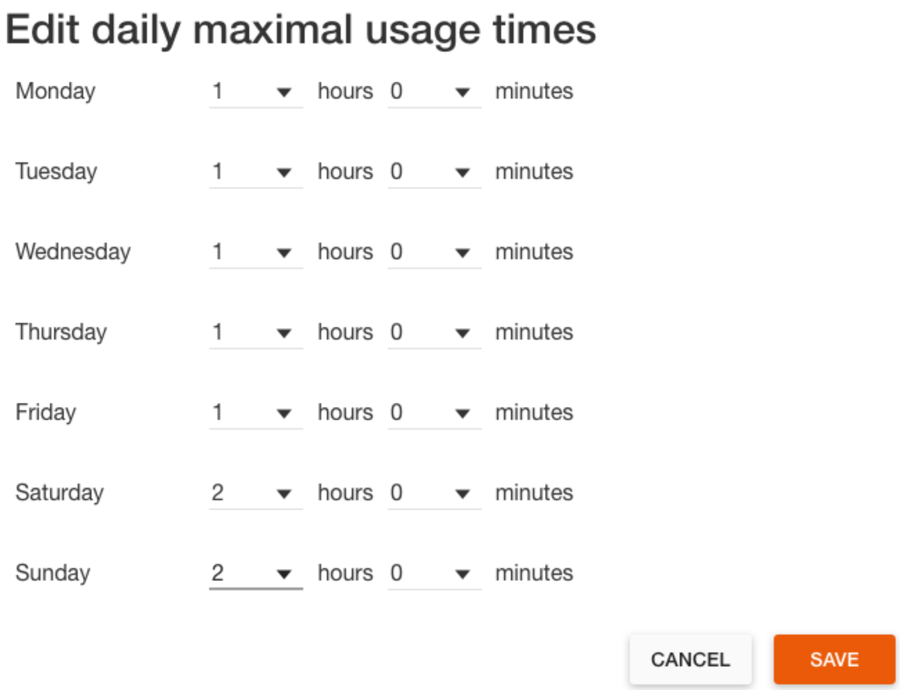
8.2.10 Limit the maximum Internet usage per day

In addition to the time slots, which define the time of day, when Internet usage is generally allowed, you can set a maximum internet usage time for each day of the week. So it is for example possible to allow Internet usage in the time from 7am to 8pm, but within this time restrict the Internet usage to a maximum of one hour in total.
Activate the sliding switch to restrict the maximum daily usage time:



Restrictions on daily Internet usage:

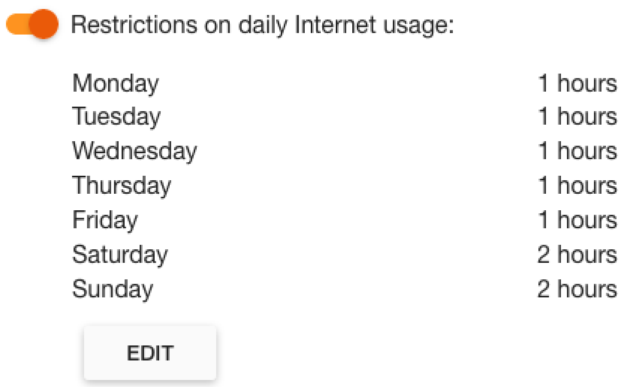
For a newly created Protection profile, the daily usage is set to 1 hour. Click on the "Edit" button to change the daily usage restrictions. The following dialog opens:



Edit daily maximal usage times

Monday	1	hours	0	minutes
Tuesday	1	hours	0	minutes
Wednesday	1	hours	0	minutes
Thursday	1	hours	0	minutes
Friday	1	hours	0	minutes
Saturday	2	hours	0	minutes
Sunday	2	hours	0	minutes

Set the maximum usage time for each day of the week and save the settings. Then the configuration is as follows:



Restrictions on daily Internet usage:

Monday	1 hours
Tuesday	1 hours
Wednesday	1 hours
Thursday	1 hours
Friday	1 hours
Saturday	2 hours
Sunday	2 hours

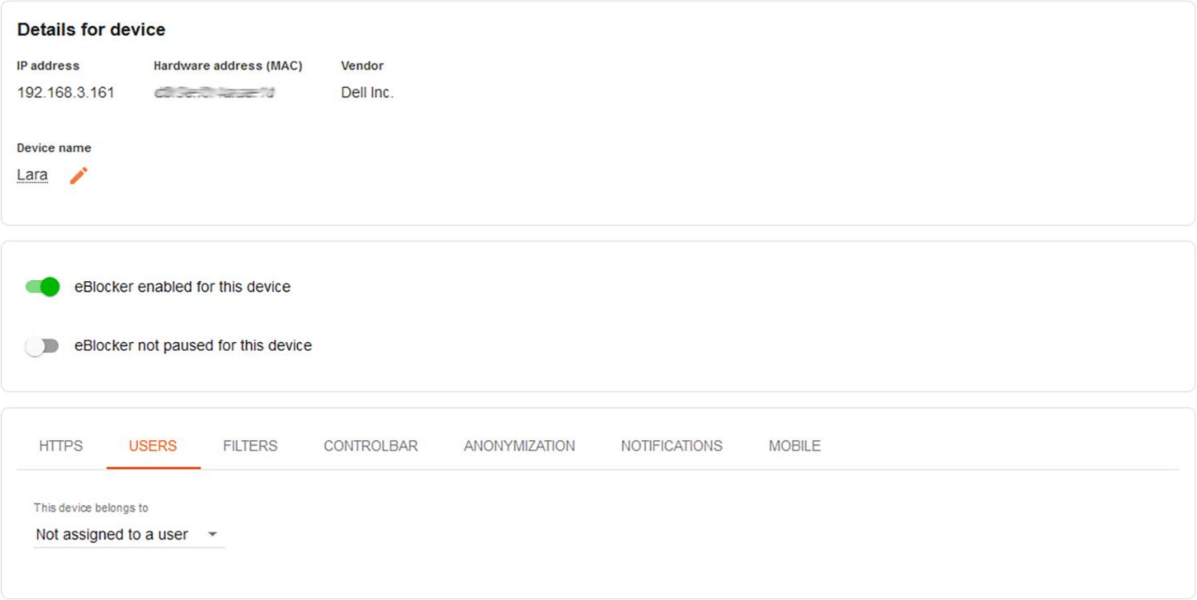
Deactivate the corresponding sliding switch to disable these restrictions completely.

Note:
The corresponding online time is available for each user individually. It is not divided among different users of the same profile.

8.2.11 Assign a user to device

To activate Parental Control for a device, a user must be assigned to that device.

Navigate to the "eBlocker Settings > Devices" (see section 8.) and click on the device to which you want to assign a user:



Details for device

IP address	Hardware address (MAC)	Vendor
192.168.3.161	[redacted]	Dell Inc.

Device name
Lara

● eBlocker enabled for this device

○ eBlocker not paused for this device

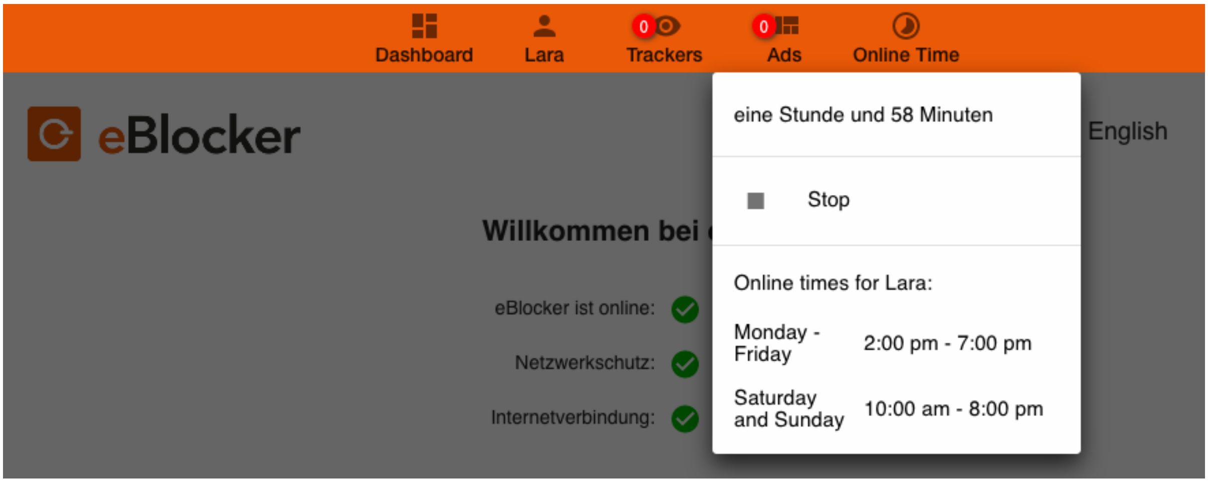
This device belongs to
Not assigned to a user

A new device is initially not assigned to a user. Click on the according selection list and select the main owner of that device. The device will immediately be subject to the restrictions as defined by the protection profile of that user.

It is possible to assign multiple devices to the same user. Then the same filter rules apply on all these devices. The Internet usage time per day is summed up for all these devices.

8.2.12 Controlbar for users with protection profiles

If a protection profile is set for a user that contains one or more parental control restrictions, this user is provided with a modified and restricted controlbar. Via the additional menu item "Online-Times" you can see the currently remaining internet usage time as well as the allowed usage times:



eine Stunde und 58 Minuten

■ Stop

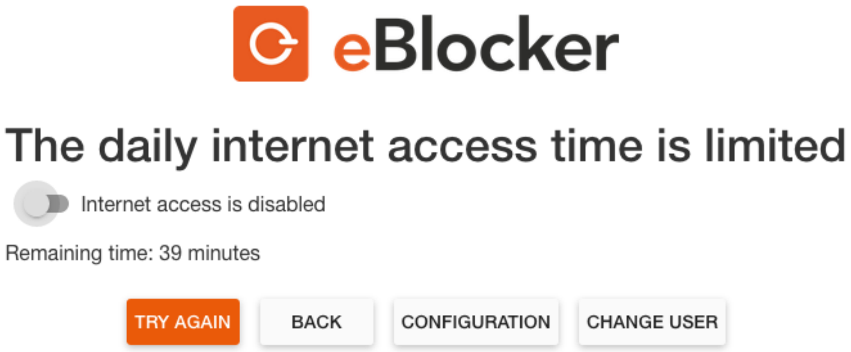
Online times for Lara:

Monday - Friday	2:00 pm - 7:00 pm
Saturday and Sunday	10:00 am - 8:00 pm

8.2.13 What happens if the daily internet usage time is limited?

If the daily Internet usage time is limited, Internet access must be activated explicitly. Otherwise, automatic processes of the operating system or other apps on the devices would unintentionally "consume" the usage time. E.g. because the apps might regularly check for updates.

Therefore, the following page is displayed when the user tries to go to any page using an Internet browser:

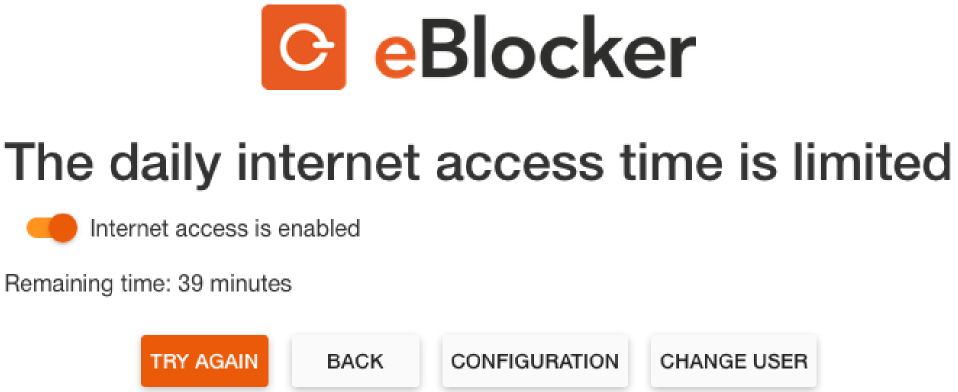


The daily internet access time is limited

Internet access is disabled

Remaining time: 39 minutes

To activate the Internet use, the sliding switch must be activated. From this moment on, the remaining usage time is correspondingly reduced. The currently remaining time is displayed to allow the user a flexible time management.



The daily internet access time is limited

Internet access is enabled

Remaining time: 39 minutes

The current remaining usage time can always be reviewed via the eBlocker icon and the controlbar. It's also possible to end internet usage via the controlbar in order to spare the remaining Internet usage time (e.g, see above: "Remaining time: 39 minutes"):

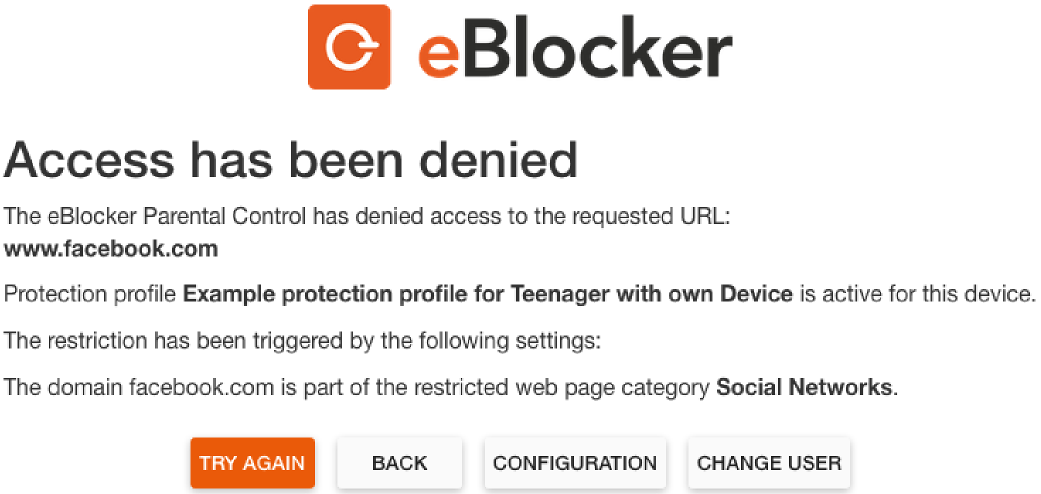
The Internet access is also automatically deactivated after a few minutes, when there are no Internet connections seen by the eBlocker. This also helps to consume the daily Internet usage time in a flexible and meaningful way.

8.2.14 What happens if the internet access is denied?

When Internet access is denied, while using an Internet browser, one of the following messages is displayed depending on the reason for blocking the Internet access. This message is displayed in order to make it clear why the Internet access was denied.

Please note that other applications and apps may not function as expected and may display unspecific error messages, when the Internet connection is blocked. Displaying a corresponding message by the eBlocker is in most cases not possible with such applications.

Restriction through category filter:
If access to a site has been disabled due to a site category filter, the user will see the following message from the eBlocker instead of the desired site:



Access has been denied

The eBlocker Parental Control has denied access to the requested URL:
www.facebook.com

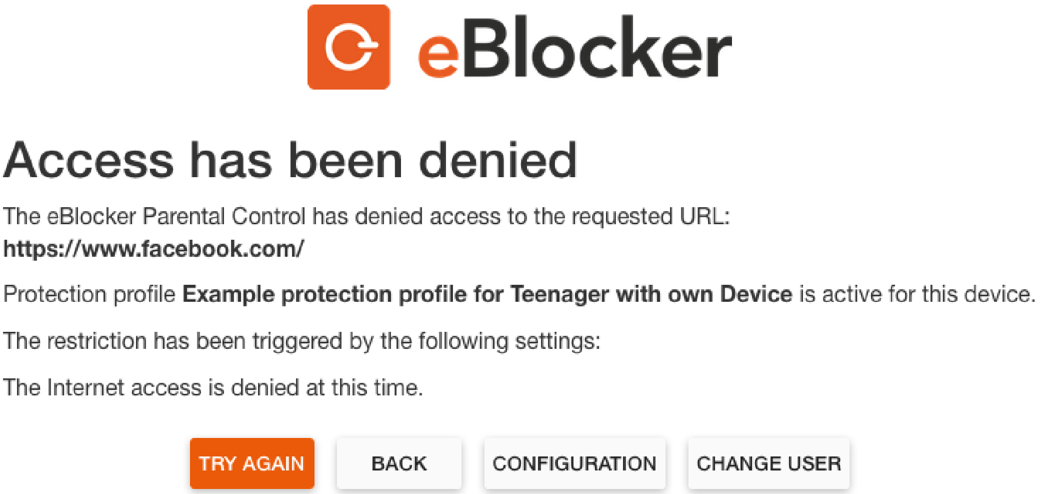
Protection profile **Example protection profile for Teenager with own Device** is active for this device.

The restriction has been triggered by the following settings:

The domain facebook.com is part of the restricted web page category **Social Networks**.

Via the button "Configuration" the Parental Control settings can be accessed directly. Of course the administrator password is required to do so (see section 8.1.3).
The active user of the device can be changed via the button "Change user". If the new user is subject to another protection profile, access to the page might or might not be allowed, depending on that other profkle. In any case, the corresponding user PIN must be entered to switch to another user.

Restriction of access outside of allowed time slots:
If access to a website takes place outside an allowed time slot, the user will see the following message from the eBlocker instead of the desired Web site:



Access has been denied

The eBlocker Parental Control has denied access to the requested URL:
https://www.facebook.com/

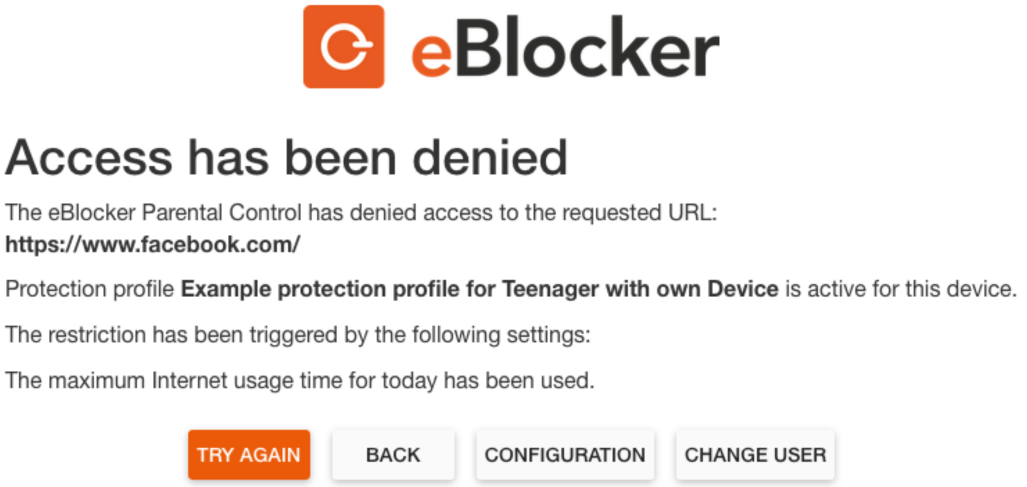
Protection profile **Example protection profile for Teenager with own Device** is active for this device.

The restriction has been triggered by the following settings:

The Internet access is denied at this time.

The "Configuration" and "Change user" buttons have the same function as described above.

If the maximum usage time per day has been reached:
If a maximum usage time per day is set and has already been reached, the following message is displayed:



Access has been denied

The eBlocker Parental Control has denied access to the requested URL:
https://www.facebook.com/

Protection profile **Example protection profile for Teenager with own Device** is active for this device.

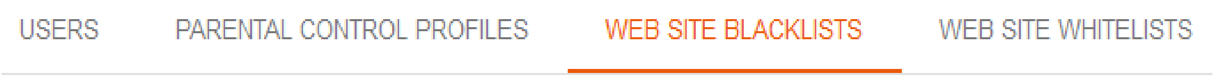
The restriction has been triggered by the following settings:

The maximum Internet usage time for today has been used.

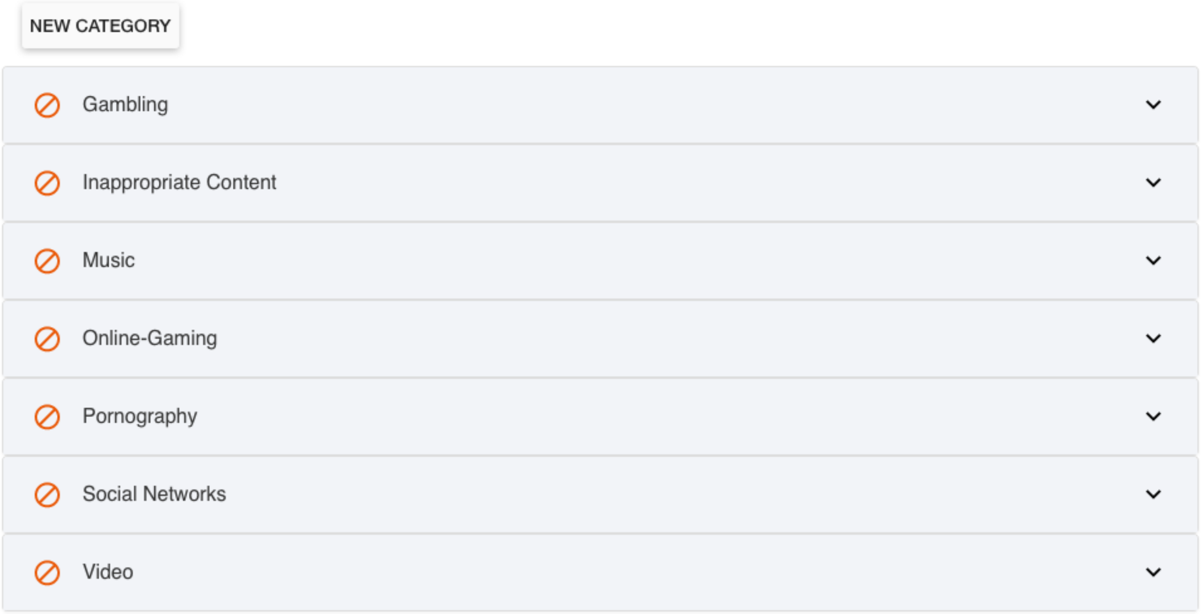
The "Configuration" and "Change user" buttons have the same function as described above.

8.2.15 Add own lists to the Blacklists

Navigate to the "eBlocker Settings > Parental Control" menu and click on the page “Website Blacklist”:

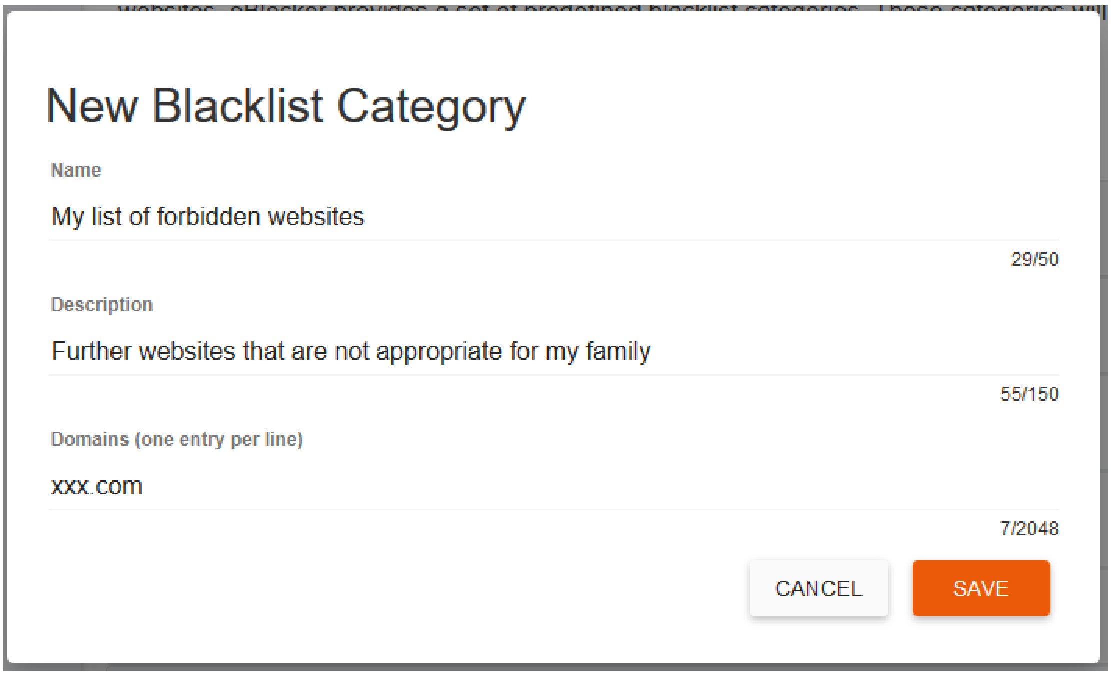


The eBlocker aready provides a set of predefined blacklist categories:



- Gambling
- Inappropriate Content
- Music
- Online-Gaming
- Pornography
- Social Networks
- Video

You can create additional categories with lists of disallowed websites at any time and use them in the protection profile. Click on the button "New category". The following dialog opens:



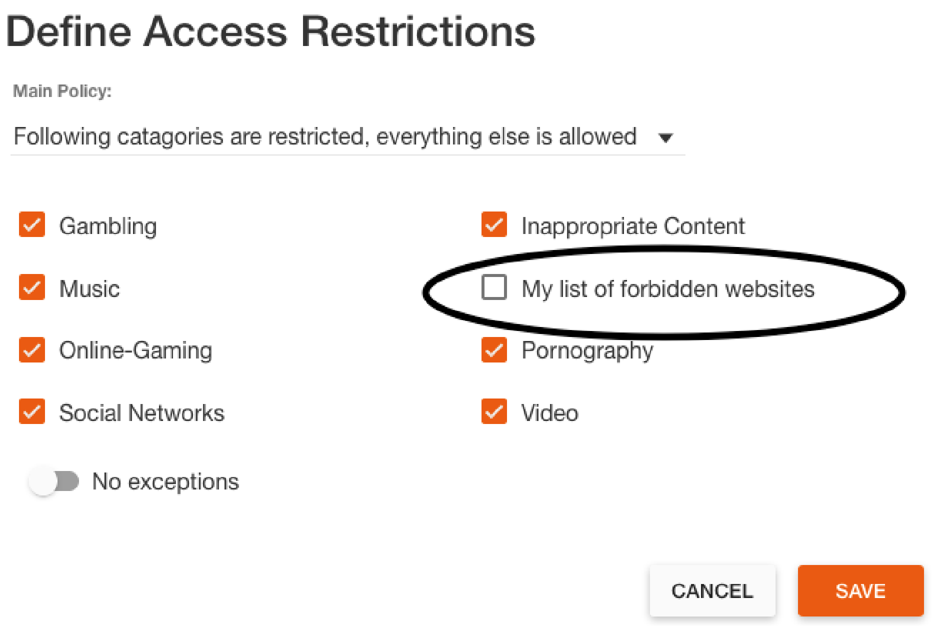
New Blacklist Category

Name
My list of forbidden websites
29/50

Description
Further websites that are not appropriate for my family
55/150

Domains (one entry per line)
xxx.com
7/2048

You can view, add, or remove your own blacklist categories at any time. All your own categories can be selected in the Protection profiles together with the already provided categories (see section 8.2.8.):



Define Access Restrictions

Main Policy:
Following catagories are restricted, everything else is allowed

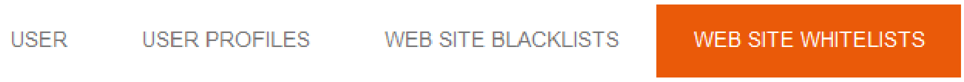
☑ Gambling
☑ Music
☑ Online-Gaming
☑ Social Networks
☑ Inappropriate Content
☐ My list of forbidden websites
☑ Pornography
☑ Video

No exceptions

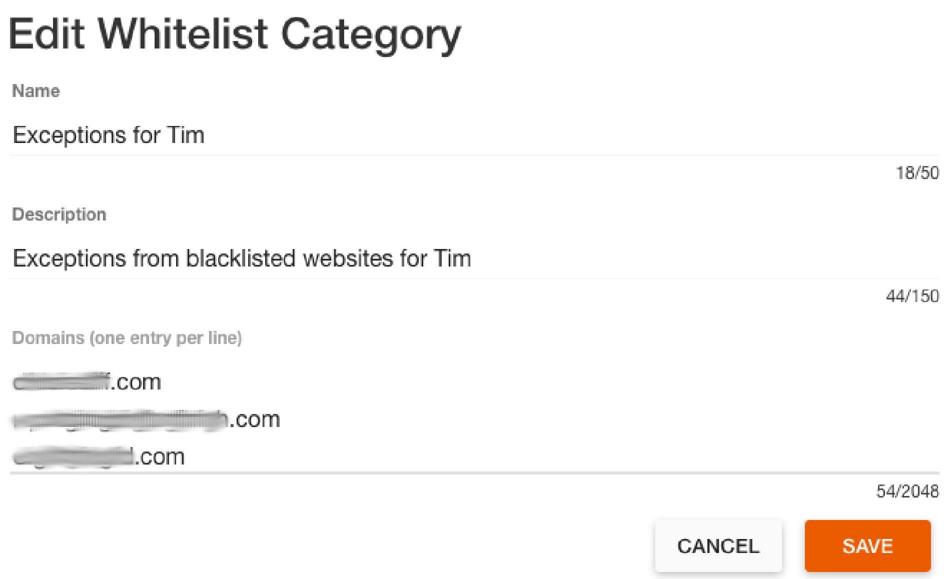
8.2.16 Add whitelists to blacklist categories

The provided blacklist categories are very comprehensive and are updated regularly. It is, of course, possible that the lists are too strict in some cases and deny access to websites that your children need and should receive access to.
To avoid having to disable the entire protection category just because of a few websites, you can define exceptions from the standard categories by defining categories of explicitly allowed websites – also called “whitelists”

Navigate to the "eBlocker Settings > Parental Control" menu and select the page "Website Whitelists”:



Create a whitelist category with websites for which you want to explicitly allow access. Initially, the list of categories with allowed sites is empty. Click on the button "New Category" to create a new category:

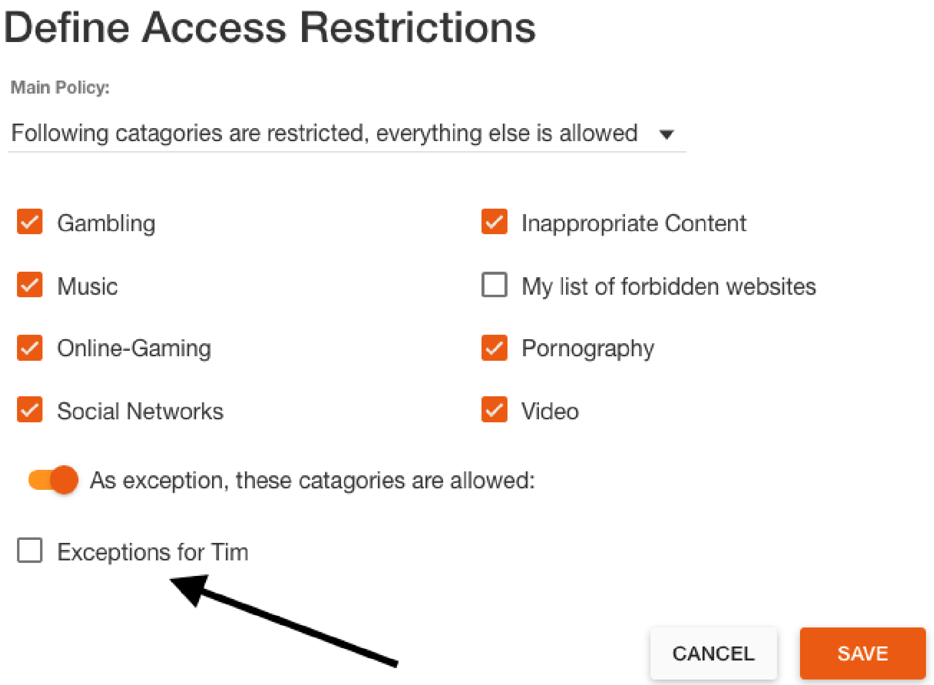

Edit Whitelist Category

Name
Exceptions for Tim
18/50

Description
Exceptions from blacklisted websites for Tim
44/150

Domains (one entry per line)
[redacted].com
[redacted].com
[redacted].com
54/2048

Once you have created one or more categories with explicitely allowed websites, these appear as possible exceptions in the configuration of the protection profiles (see section 8.2.8):



Define Access Restrictions

Main Policy:

Following catagories are restricted, everything else is allowed ▾

☑ Gambling

☑ Music

☑ Online-Gaming

☑ Social Networks

☑ Inappropriate Content

□ My list of forbidden websites

☑ Pornography

☑ Video

● As exception, these catagories are allowed:

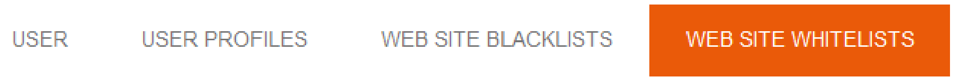
□ Exceptions for Tim

Activate the exception slider switch and select the exception/whitelist categories you want to use in this profile.

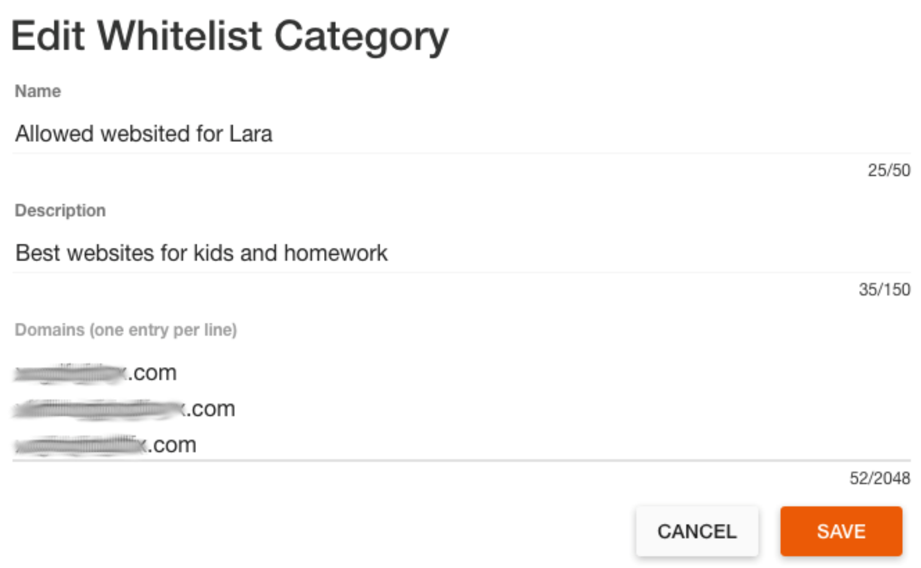
8.2.17 Add own whitelist categories

Rather than restrict Internet access through categories of blacklists, you can also work with categories of explicitly allowed sites. Everything that is not expressly allowed is then automatically forbidden.

Navigate to the "eBlocker Settings > Parental Control" menu and click on the page "Websites Whitelists:



Create one or more categories of explicitly allowed sites:



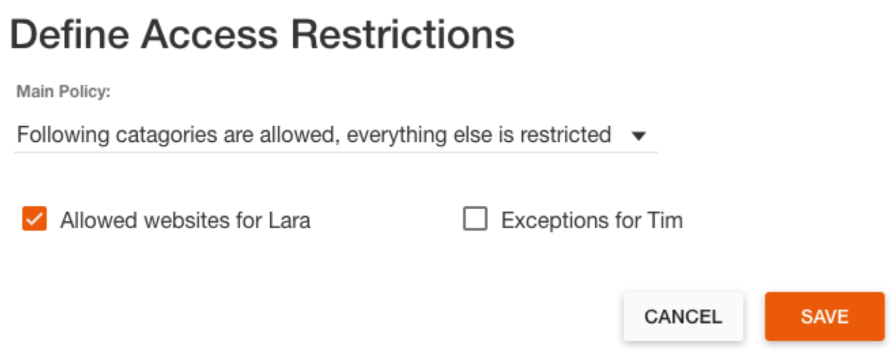
Edit Whitelist Category

Name: Allowed websited for Lara (25/50)

Description: Best websites for kids and homework (35/150)

Domains (one entry per line):
[redacted].com
[redacted].com
[redacted].com
(52/2048)

You can use these whitelist categories, when creating a protection profile. In order to work with explicitly allowed websites, you must change the main policy in the access restriction dialog from "Following catagories are restricted, everything else is allowed" to "Following catagories are allowed, everything else is restricted":



Define Access Restrictions

Main Policy: Following catagories are allowed, everything else is restricted ▾

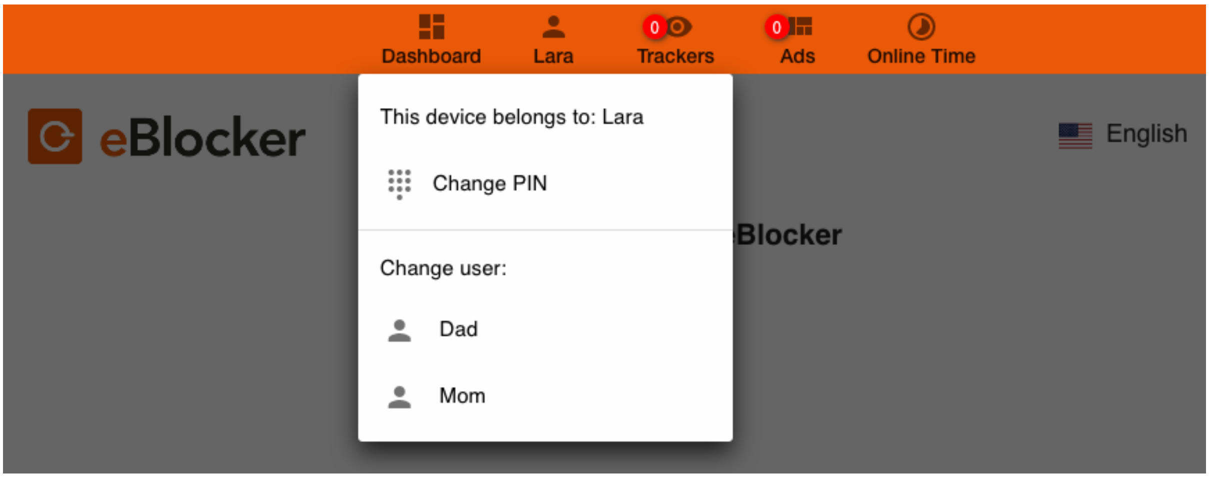
☑ Allowed websites for Lara
□ Exceptions for Tim

Note that Internet access through such profiles can be very limited. So it may not be possible to load operating system updates, and many apps will likely not work as usual.

8.2.18 Change of user through controlbar

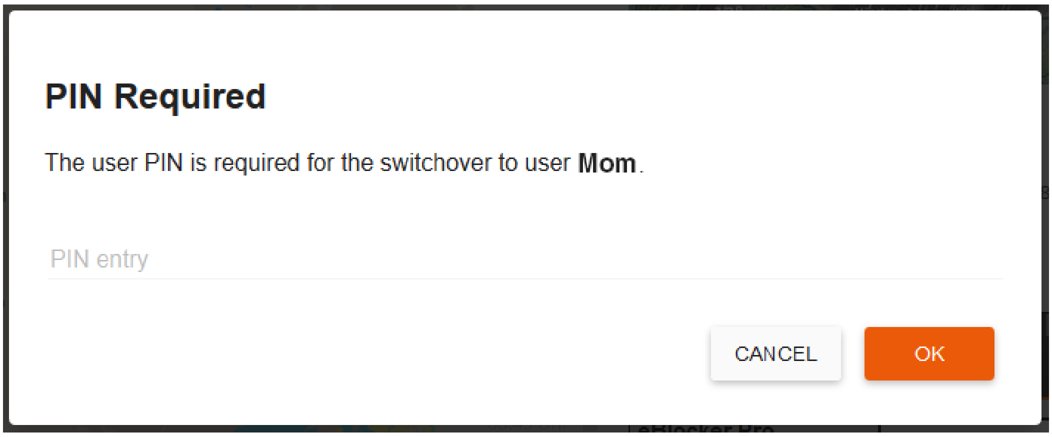
If a PIN has been assigned to one or more users (see section 8.2.4), the current user of a device can be changed via the controlbar. Through the change of the user, the respectively active protection profile might also change. Thus changing or even disabling the access restrictions of a device can be very simple.

Suppose **Dad**, and **Mom** have a user PIN, but **Tim** and **Lara** do not. Then the controlbar on Lara’s device would look like this:



This device belongs to: Lara

The adults can temporarily take ownership of the device by entering the PIN and thereby temporarily remove the protection restrictions:



PIN Required

The user PIN is required for the switchover to user **Mom**.

After the device switchover the controlbar looks like this:

The controlbar always shows the current user as well as the main user of the device. If the device is currently used ba a different user, then it can be returned to the main user by selecting “Return device”. If the main user himself has set a PIN, the PIN is required for the return. Additional functions are available to users with PIN:

- Lock Internet access for the device. Only a user with PIN can remove the lock.
- Change own PIN.

8.2.19 Migration of Parental Control to eBlockerOS 1.0

If you have already used Parental Control in eBlockerOS 1.0, you will notice that users have been created for each protection profile in use. These users have automatically been assigned to the appropriate devices.

This was necessary because the profiles are no longer directly assigned to the devices.

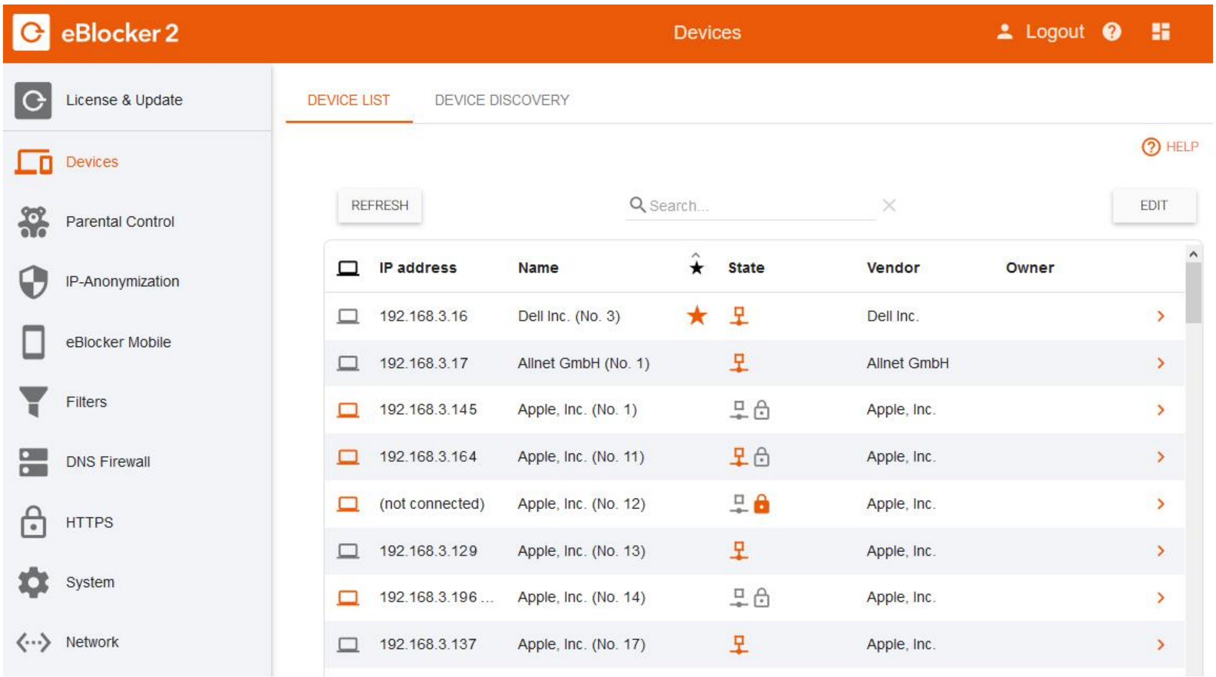
Nothing should have changed in your home network, due to the upgrade.

In order to make the best of Parental Control, you should rename or replace the automatically created users and add more, if necessary.

8.3 Devices

Available for **eBlocker Base**, **eBlocker Pro** and **eBlocker Family**

The „Device“ function shows a list of all network devices that are identified by your eBlocker in your home network.



IP address	Name	★	State	Vendor	Owner
192.168.3.16	Dell Inc. (No. 3)	★		Dell Inc.	
192.168.3.17	Allnet GmbH (No. 1)			Allnet GmbH	
192.168.3.145	Apple, Inc. (No. 1)		🔒	Apple, Inc.	
192.168.3.164	Apple, Inc. (No. 11)		🔒	Apple, Inc.	
(not connected)	Apple, Inc. (No. 12)		🔒	Apple, Inc.	
192.168.3.129	Apple, Inc. (No. 13)			Apple, Inc.	
192.168.3.196 ...	Apple, Inc. (No. 14)		🔒	Apple, Inc.	
192.168.3.137	Apple, Inc. (No. 17)			Apple, Inc.	

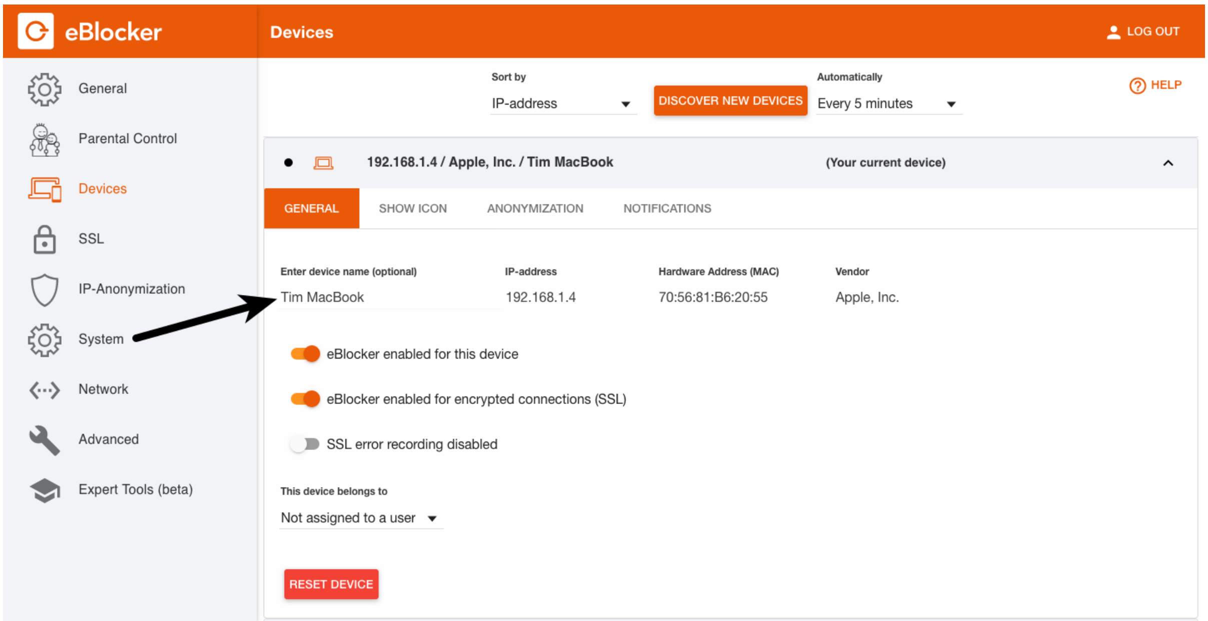
The devices are initially identified by their IP address and - as far as the eBlocker can determine - by the manufacturer. By clicking on the IP address, you open further details about the device and can adjust the settings.

Your router and eBlocker have their own grey icon. You can assign an optional name to both devices, but you cannot make any other settings.

Devices with an orange icon are online are currently active on your network.

Devices with a grey icon are currently not active in your network.

8.3.1 Devices



Sort by: IP-address

Automatically: Every 5 minutes

● 192.168.1.4 / Apple, Inc. / Tim MacBook (Your current device)

Enter device name (optional)	IP-address	Hardware Address (MAC)	Vendor
Tim MacBook	192.168.1.4	70:56:81:B6:20:55	Apple, Inc.

eBlocker enabled for this device

eBlocker enabled for encrypted connections (SSL)

SSL error recording disabled

This device belongs to: Not assigned to a user

8.3.2 Devices - Name

We recommend assigning a device name to all devices so that you can easily recognize them at any time (e. g."Christian's laptop", "Living room TV" or "Sabine's smartphone").

The IP address, the hardware address (MAC) and, if available, the manufacturer per device are also displayed here.

8.3.3 Devices - Activate eBlocker

By default, the eBlocker is automatically activated for most devices. Only some device types (e. g. some IP phones and Hi-Fi components) are deactivated in the default setting. Devices for which the eBlocker is activated are displayed with an orange icon.

You can define at any time whether or not the eBlocker should analyze each device individually. If the eBlocker has been activated for the device, further function are available below.

8.3.4 Devices - Activate HTTPS

If the HTPS function on the eBlocker have been activated in general (see section **Fehler! Verweisquelle konnte nicht gefunden werden.**), you can instruct the eBlocker to monitor encrypted connections (HTTPS) for each device individually.

8.3.5 Devices - User

eBlocker Family customers can determine whether the device should be assigned to a certain user.

8.3.6 Devices – Blocker

Here you can decide whether the eBlocker should not block trackers and ads, whether the eBlocker should use its "Domain Blocker", or whether the eBlocker should use its "Pattern Blocker". The "Pattern Blocker" setting preempts the activation of the HTTPS function.

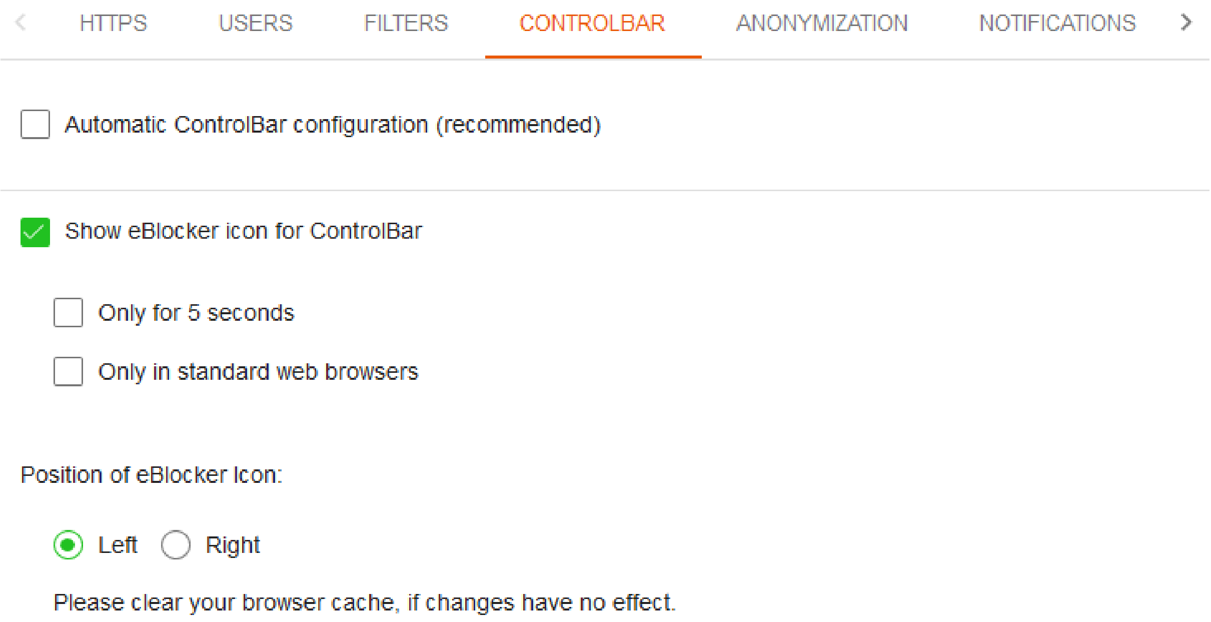
If you set the setting to Automatic, the eBlocker will use the HTTPS function (enabled or disabled) to decide for you whether to use the domain or pattern blocker. The setting "Automatic" is our recommendation.

8.3.7 Devices – Controlbar

Here you can specify whether the eBlocker icon (see section 7.1) should always, never or only briefly be displayed for five seconds on the device when you access a new web page.

Additionally, there is the option to show the eBlocker icon only in standard browsers like Microsoft Edge, Firefox, Chrome, or Safari. This also includes browsers based on Chrome or Firefox. For example, the eBlocker icon will not appear in apps.

Here you can also set the position of the eBlocker icon.



□ Automatic ControlBar configuration (recommended)

☑ Show eBlocker icon for ControlBar

□ Only for 5 seconds

□ Only in standard web browsers

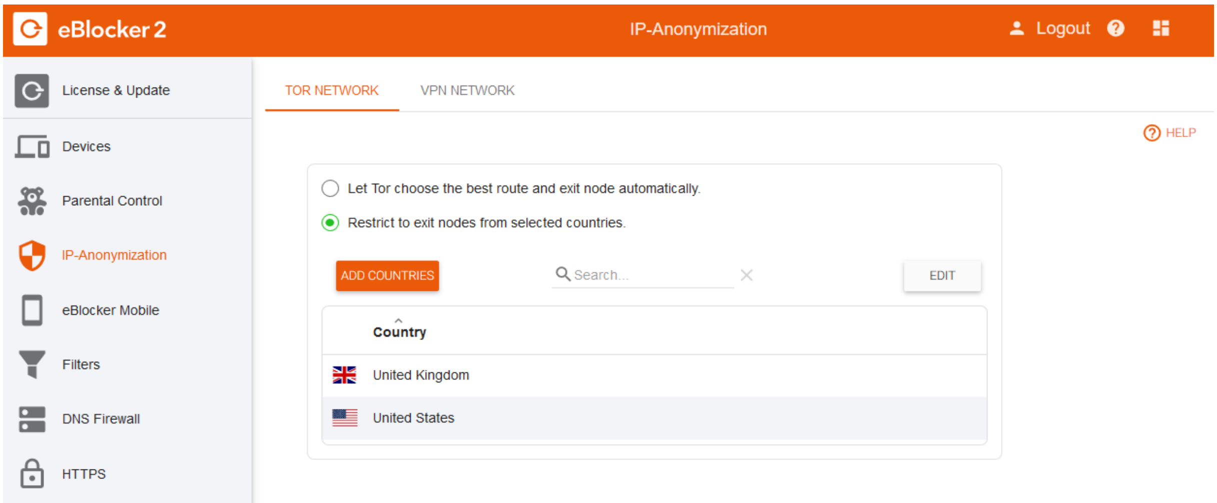
Position of eBlocker Icon:

● Left ○ Right

Please clear your browser cache, if changes have no effect.

8.3.8 Devices – Anonymization

Here you can activate IP anonymization and determine whether you want to use a Tor or VPN connection. You can also specify the cloaking for a device here. Open the selection and select one of the predefined cloaking (user agents) or enter your own user agent (see Section 7.6).

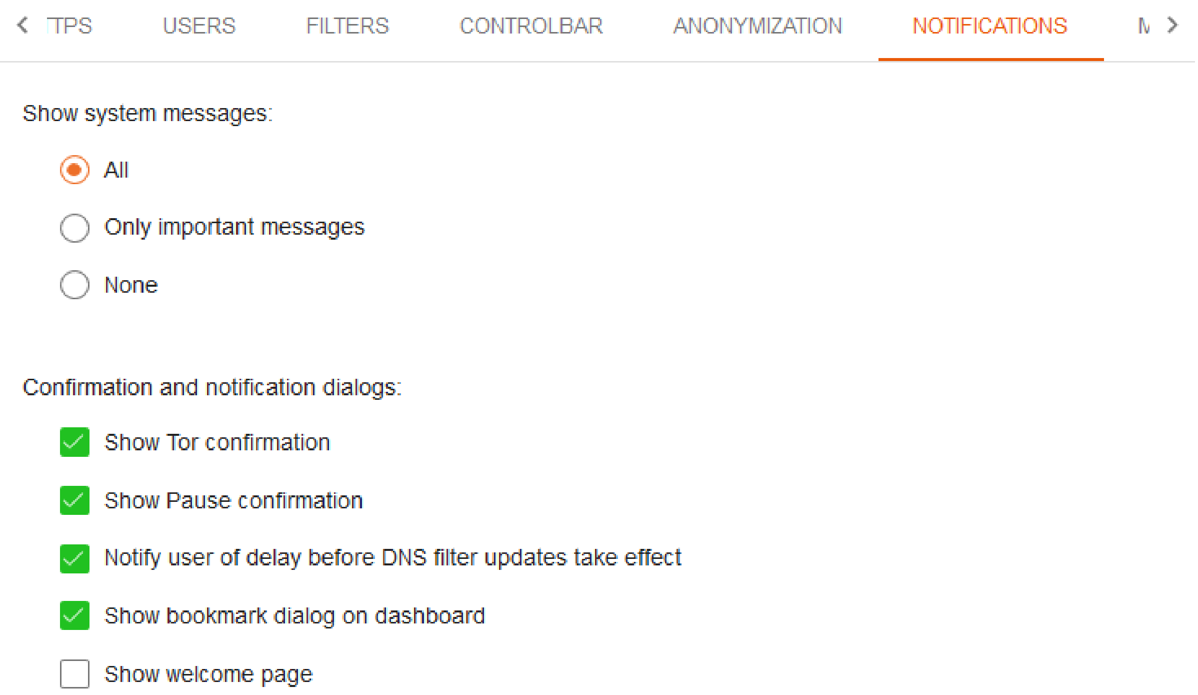


○ Let Tor choose the best route and exit node automatically.

● Restrict to exit nodes from selected countries.

Country
United Kingdom
United States

8.3.9 Devices - Notifications



Show system messages:

● All

○ Only important messages

○ None

Confirmation and notification dialogs:

☑ Show Tor confirmation

☑ Show Pause confirmation

☑ Notify user of delay before DNS filter updates take effect

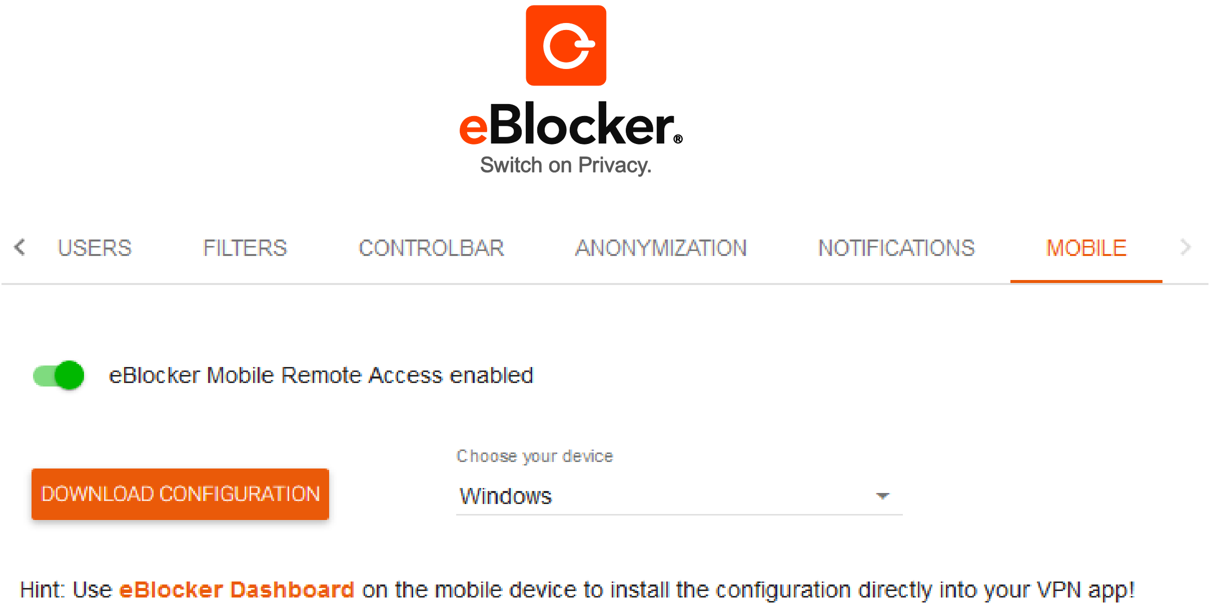
☑ Show bookmark dialog on dashboard

□ Show welcome page

8.3.10 Devices – Mobile

Here you can - if the eBlocker Mobile feature has been activated - activate access to your eBlocker for this device from outside your network.

You can determine whether this device is only activated for Internet access then, or whether eBlocker can also be configured from the device from outside your network.

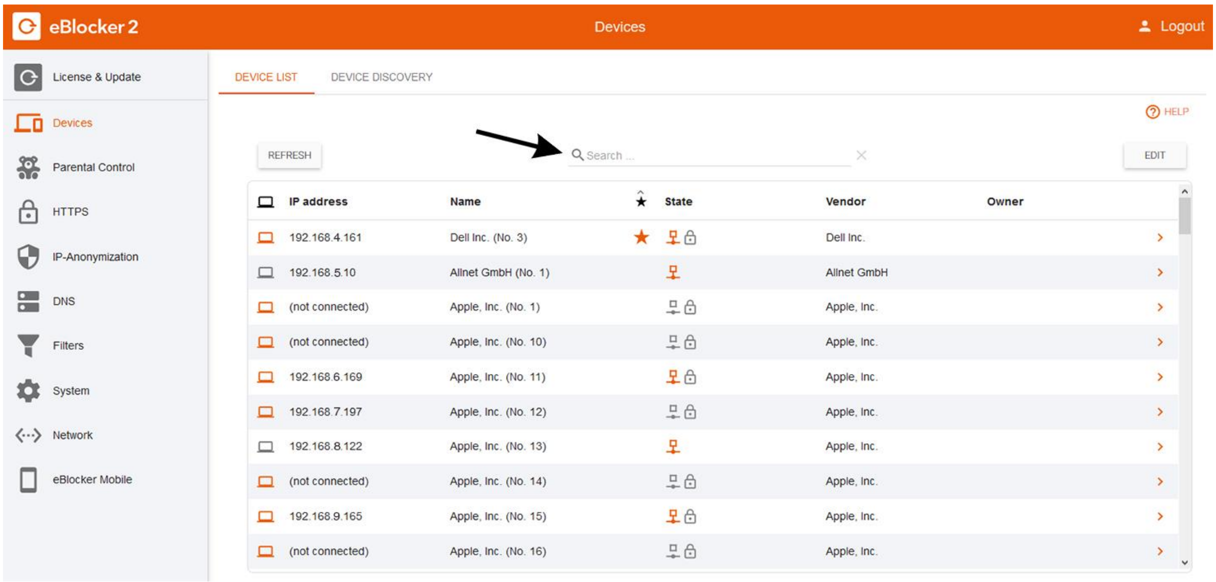


eBlocker Mobile Remote Access enabled

Choose your device: Windows

Hint: Use **eBlocker Dashboard** on the mobile device to install the configuration directly into your VPN app!

8.3.11 Devices – Detect new devices or remove devices from the list



IP address	Name	★	State	Vendor	Owner
192.168.4.161	Dell Inc. (No. 3)	★	🖧 🔒	Dell Inc.	
192.168.5.10	Allnet GmbH (No. 1)		🖧	Allnet GmbH	
(not connected)	Apple, Inc. (No. 1)		🖧 🔒	Apple, Inc.	
(not connected)	Apple, Inc. (No. 10)		🖧 🔒	Apple, Inc.	
192.168.6.169	Apple, Inc. (No. 11)		🖧 🔒	Apple, Inc.	
192.168.7.197	Apple, Inc. (No. 12)		🖧 🔒	Apple, Inc.	
192.168.8.122	Apple, Inc. (No. 13)		🖧	Apple, Inc.	
(not connected)	Apple, Inc. (No. 14)		🖧 🔒	Apple, Inc.	
192.168.9.165	Apple, Inc. (No. 15)		🖧 🔒	Apple, Inc.	
(not connected)	Apple, Inc. (No. 16)		🖧 🔒	Apple, Inc.	

8.4 HTTPS

Available for **eBlocker Pro** and **eBlocker Family**

SSL stands for Secure Sockets Layer and is a protocol used to encrypt communication "end-to-end" between two communication partners. Sometimes you may also encounter the abbreviation TLS (TLS stands for Transport Layer Security). It is basically the same as SSL. If the standard Web protocol HTTP is encrypted using SSL, it is called HTTPS. You can recognize an encrypted loaded page by the URL starting with https:// Many browsers also display a green lock in the address bar.
Many websites, especially those of banks and online shops, are now protected with SSL encryption. This way you can be sure that you are actually communicating with the provider whose URL you have accessed and that no third party can change or read your entered data. However, not only reputable shops and banks use SSL. Tracking and advertising providers are also increasingly collecting their data via HTTPS/SSL. Your profile data is then sent to the tracking server in encrypted form, but of course this does not prevent the data collector from continuing to create a detailed profile of you.

Once HTTPS support is enabled in eBlocker, each eBlocker generates a unique device root certificate and a private key. This certificate is used to encrypt communication between your device and the eBlocker when the eBlocker loads an SSL-protected web page.

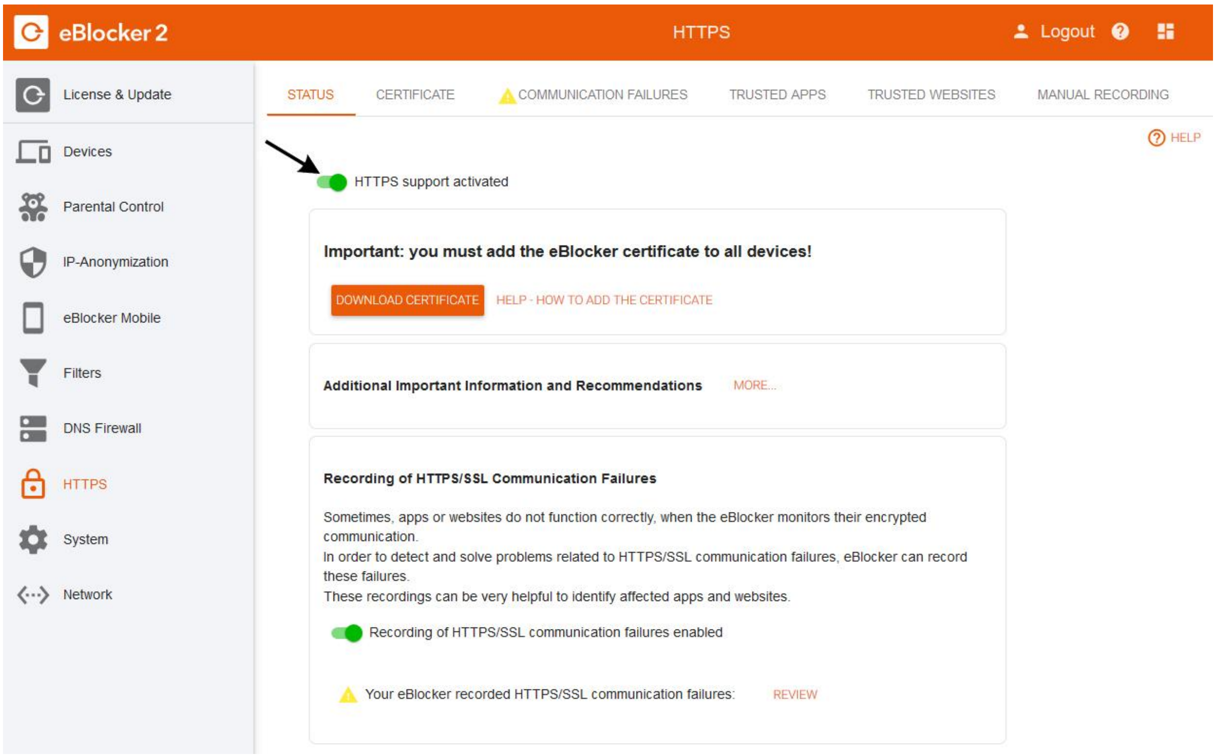
Once HTTPS is activated, the eBlocker terminates the encrypted connection so that the data stream can be analyzed. The eBlocker is the end of "end-to-end encryption". Since the browser expects an encrypted connection with HTTPS, the eBlocker then encrypts the communication to your end device. To do this, it is necessary to first include the so-called security certificate of your eBlocker in your operating system and then, if necessary, in the browsers with its own certificate store as described in Section 6.2. This certificate is sometimes also called a certificate for certification authorities, a root certificate, or a root certificate.

We have no access to your private key or your device and have done everything to protect the eBlocker from hackers - but of course there is no 100 percent security. We offer SSL support as an option. If you feel uncomfortable with the eBlocker decrypting the HTTPS connection, please do not activate this option.

Or add the websites you trust and you don't want eBlocker to look into the list of trusted websites. On these pages, for example, the eBlocker cannot detect and block trackers, and the eBlocker icon cannot be displayed either (see also Section 8.4.5).

8.4.1 HTTPS Status

To activate SSL, click on the eBlocker icon in the upper right corner of your browser window and go to "Settings". Click on the menu item "HTTPS".
You are now in the "Status" tab. Activate the HTTPS function for your eBlocker by moving the button to the right.



HTTPS support activated

Important: you must add the eBlocker certificate to all devices!

Additional Important Information and Recommendations

Recording of HTTPS/SSL Communication Failures

Sometimes, apps or websites do not function correctly, when the eBlocker monitors their encrypted communication.
In order to detect and solve problems related to HTTPS/SSL communication failures, eBlocker can record these failures.
These recordings can be very helpful to identify affected apps and websites.

Recording of HTTPS/SSL communication failures enabled

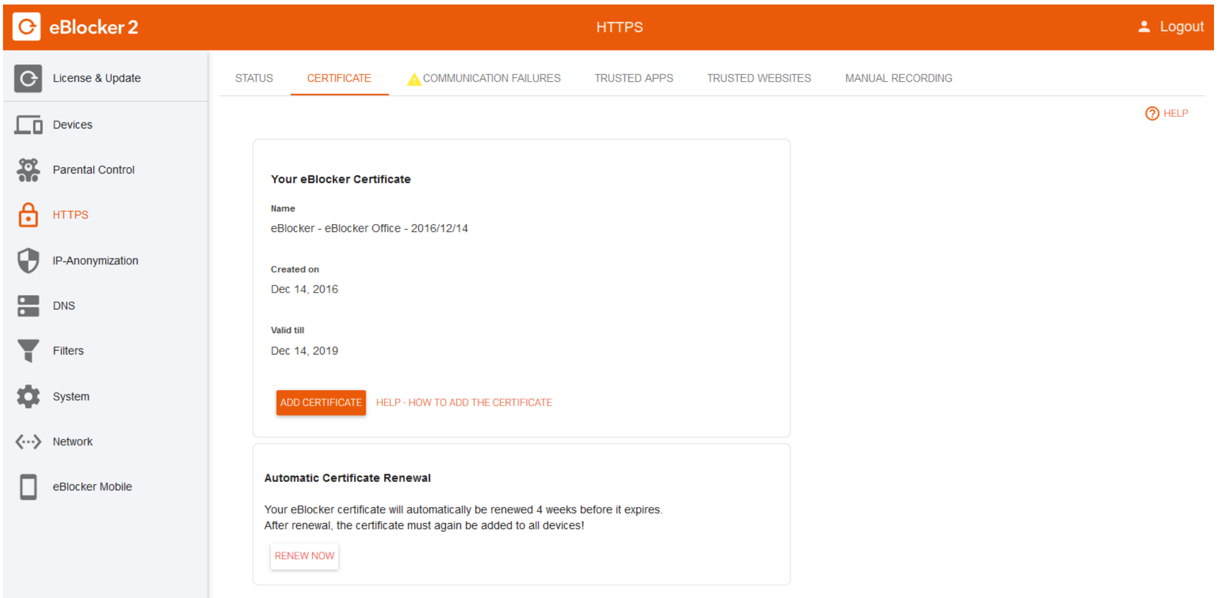
Your eBlocker recorded HTTPS/SSL communication failures:

Please note that the certificate must first be stored in your operating system and then, if necessary, in browsers with their own certificate store. See Chapter 6.2 "Adding the eBlocker certificate".
Click on "Help - how to add the certificate to your browser" for a detailed explanation of how to add the certificate.

Some apps or websites do not work correctly when the eBlocker monitors their encrypted communication. If you activate the "Recording connection errors" function, eBlocker records the problematic connections. These records can be very helpful in identifying affected apps and websites.

8.4.2 HTTPS Certificate

Here you can see some information about your eBlocker certificate, can add the eBlocker certificate, or renew it.



Your eBlocker Certificate

Name
eBlocker - eBlocker Office - 2016/12/14

Created on
Dec 14, 2016

Valid till
Dec 14, 2019

Automatic Certificate Renewal

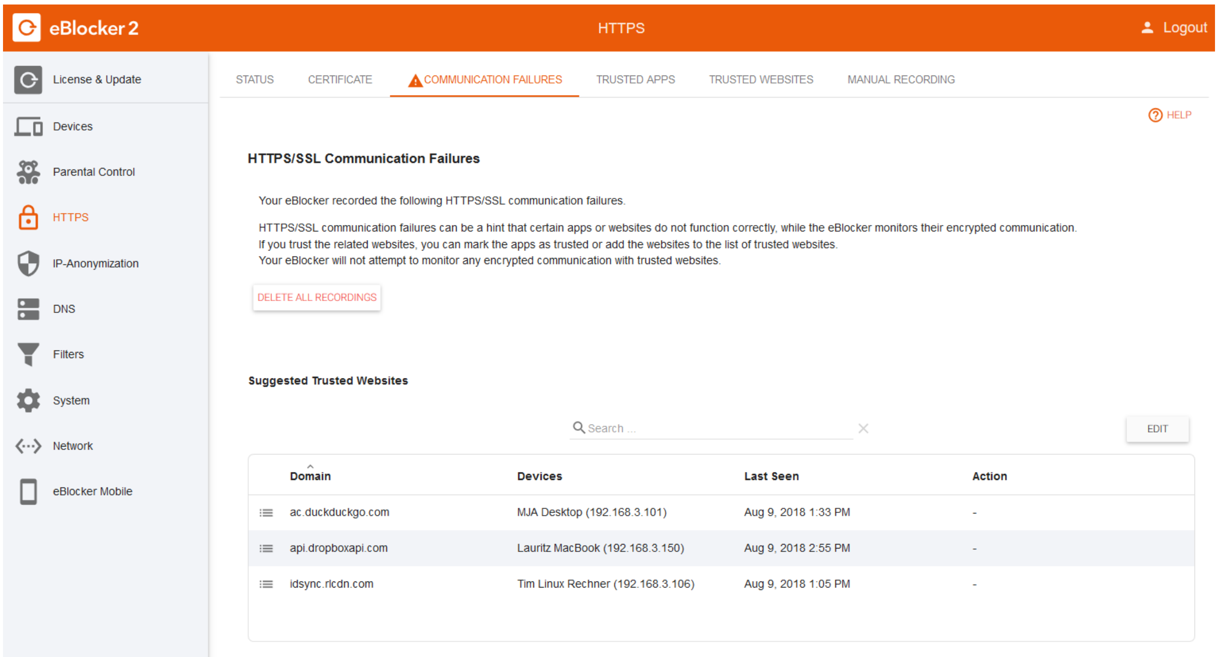
Your eBlocker certificate will automatically be renewed 4 weeks before it expires.
After renewal, the certificate must again be added to all devices!

Please note that the certificate must first be stored in your operating system and then, if necessary, in browsers with their own certificate store. See Chapter 6.2 "Adding the eBlocker certificate".
Click on "Help - how to add the certificate to your browser" for a detailed explanation of how to add the certificate.

Your eBlocker certificate will be automatically renewed 4 weeks before it expires. However, you can renew the eBlocker certificate yourself at any time. Click on the button "Renew now" and follow the wizard that will help you to create the new version. Please note, however, that you must then store the new eBlocker certificate again for all devices.

8.4.3 HTTPS/SSL connection error

If you have activated the "Recording connection errors" function, you may see a list of connection errors here.



HTTPS/SSL Communication Failures

Your eBlocker recorded the following HTTPS/SSL communication failures.

HTTPS/SSL communication failures can be a hint that certain apps or websites do not function correctly, while the eBlocker monitors their encrypted communication.
If you trust the related websites, you can mark the apps as trusted or add the websites to the list of trusted websites.
Your eBlocker will not attempt to monitor any encrypted communication with trusted websites.

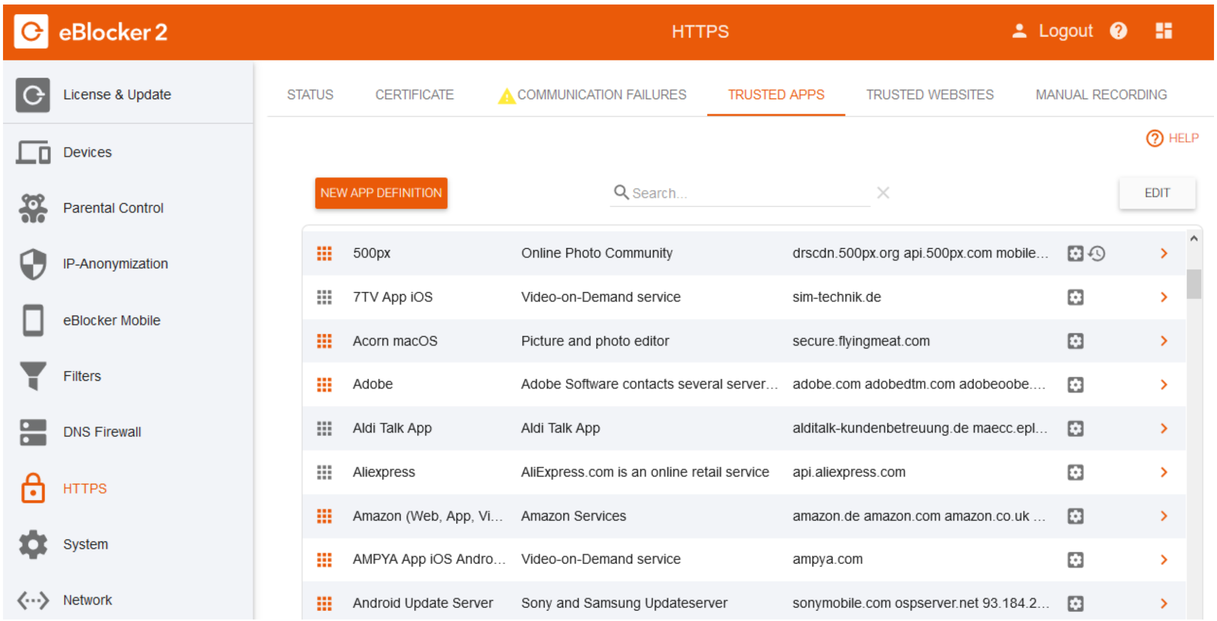
Suggested Trusted Websites

Domain	Devices	Last Seen	Action
ac.duckduckgo.com	MJA Desktop (192.168.3.101)	Aug 9, 2018 1:33 PM	-
api.dropboxapi.com	Lauritz MacBook (192.168.3.150)	Aug 9, 2018 2:55 PM	-
idsync.rlcdn.com	Tim Linux Rechner (192.168.3.106)	Aug 9, 2018 1:05 PM	-

You can easily add the found connection errors to an app exception list ("trusted app"), or set it as a "trusted website" by selecting the found domain and then selecting one of the following three options.

8.4.4 HTTPS - Trusted Apps

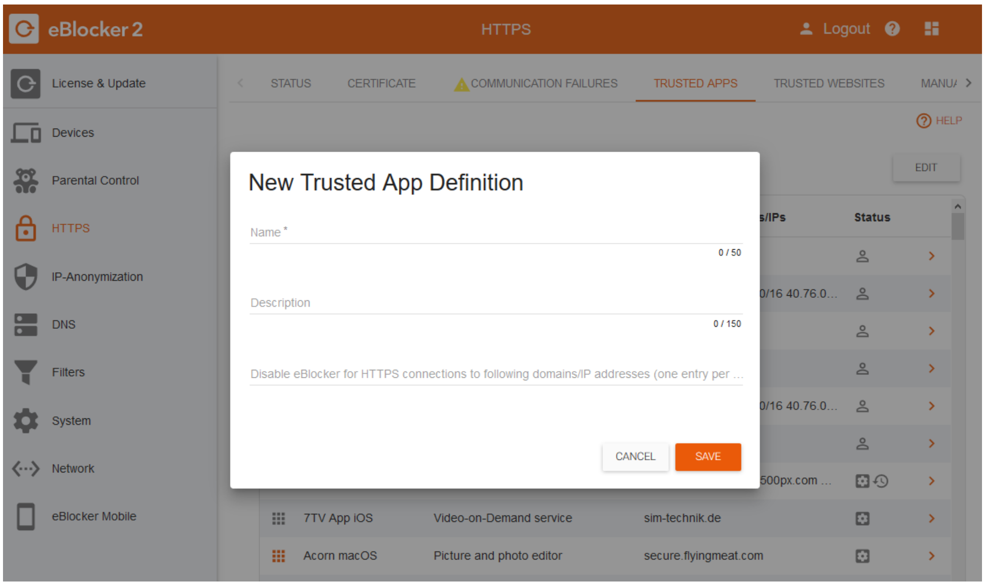
If individual apps are not compatible with eBlocker, you can exclude websites that are addressed by these apps (often unnoticed in the background) from eBlocker protection.



500px	Online Photo Community	drscdn.500px.org api.500px.com mobile...
7TV App iOS	Video-on-Demand service	sim-technik.de
Acorn macOS	Picture and photo editor	secure.flyingmeat.com
Adobe	Adobe Software contacts several server...	adobe.com adobedtm.com adobeoobe....
Aldi Talk App	Aldi Talk App	alditalk-kundenbetreuung.de maecc.epl...
Aliexpress	AliExpress.com is an online retail service	api.aliexpress.com
Amazon (Web, App, Vi...	Amazon Services	amazon.de amazon.com amazon.co.uk ...
AMPYA App iOS Andro...	Video-on-Demand service	ampya.com
Android Update Server	Sony and Samsung Updateserver	sonymobile.com ospserver.net 93.184.2...

Here you see a series of predefined exception lists for different apps, which you can now activate or deactivate with a click on the slide switch on the right side. Some exception lists for particularly popular or important apps are already activated by default.

Please note that any activated exception list means that you cannot be protected by eBlocker on the respective websites. If no exception list has been defined for an app you are looking for, you can add it using the "Define new app" button. After a click on the button a new window appears.



New Trusted App Definition

Name *
0 / 50

Description
0 / 150

Disable eBlocker for HTTPS connections to following domains/IP addresses (one entry per ...

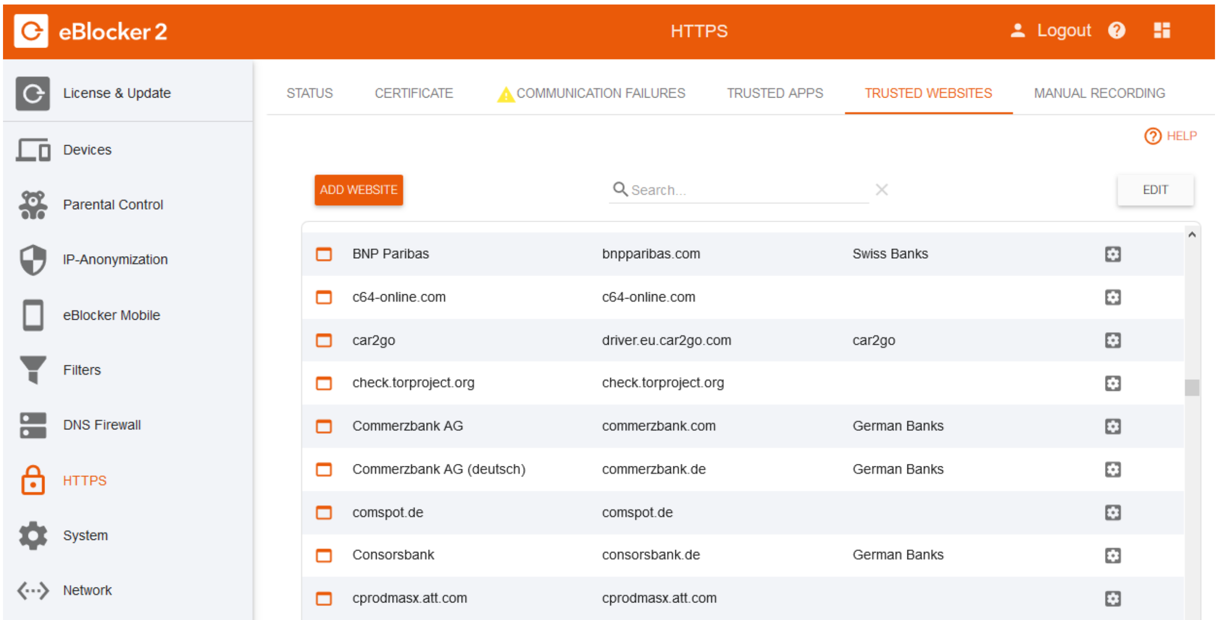
CANCEL SAVE

7TV App iOS	Video-on-Demand service	sim-technik.de
Acorn macOS	Picture and photo editor	secure.flyingmeat.com

Enter the app name and optionally add a description. The app name must be unique.
Enter one or more domains to be used by the app and not to be monitored by eBlocker. Enter one domain per line. You end a line with the Enter/Return key.
A superordinate domain automatically includes all subordinate domains.
Example: If you put the api.superapp.com domain on the exception list, calls to domains such as login.api.superapp.com are automatically excluded from eBlocker monitoring.
In rare cases it is necessary to include IP addresses in the exception list. IP addresses can be entered in the bottom field. Enter one IP address per line.
Complete the process by clicking on "Save". Your new exception list will then be saved and activated for you.

8.4.5 HTTPS - Trusted Websites

If you do not want eBlocker to work on certain encrypted websites, for example for online banking, you can add the relevant website to the SSL exception list.



BNP Paribas	bnpparibas.com	Swiss Banks
c64-online.com	c64-online.com	
car2go	driver.eu.car2go.com	car2go
check.torproject.org	check.torproject.org	
Commerzbank AG	commerzbank.com	German Banks
Commerzbank AG (deutsch)	commerzbank.de	German Banks
comspot.de	comspot.de	
Consorsbank	consorsbank.de	German Banks
cprodmasx.att.com	cprodmasx.att.com	

For example, if you do not want the eBlocker to monitor the SSL connections to your bank's Internet portal, create a corresponding entry in the SSL exception list.

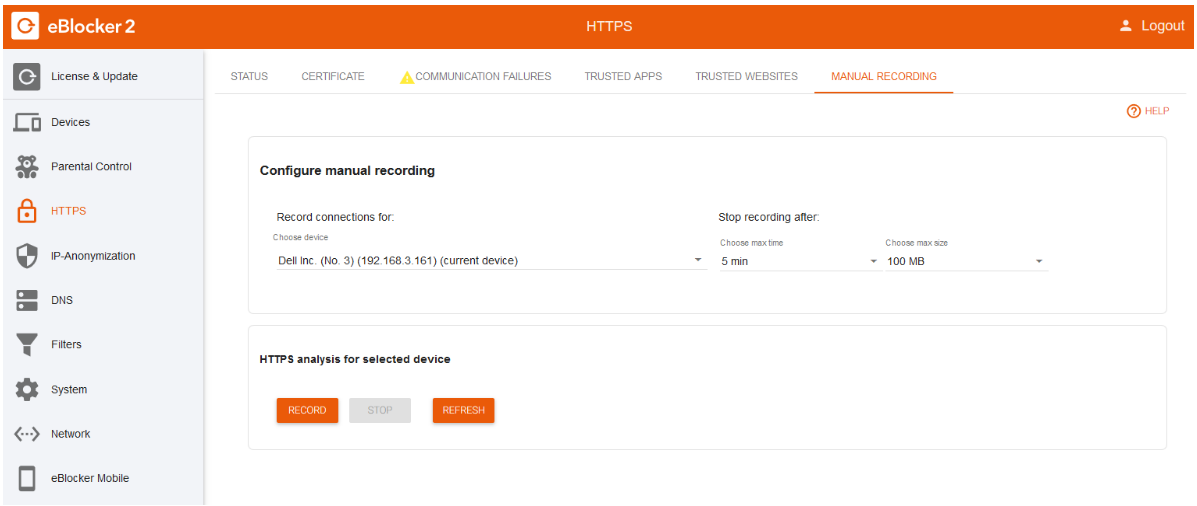
Select a unique name (e.g. "Sparkasse Hamburg"), enter the URL of the banking portal and complete the process by pressing the orange button marked "Add Domain".

Directly below the input fields you will see an exception list that has already been prepared by us. If you do not agree with one of the exempted domains, you can easily remove it by clicking on the orange trash can on the right side. Once the domain has been removed from the exception list, the eBlocker will automatically monitor calls to this site again, even if the connections are encrypted with SSL.
Important: In this exception list you also see the domains of the exception lists of the trusted apps. You cannot delete them here.

8.4.4 HTTPS – Manual Recording

"Manual Recording" is for tech savvy users only. It is used for defining domain exceptions where eBlocker should be deactivated. If an app is not compatible with eBlocker-HTTPS (see also section 5.6), the HTTPS connection requests from a device can be recorded. Afterwards eBlocker's behavior for this connection type can be defined, tested and saved as an app definition. Proceed as follows:

First analyze the HTTPS/SSL-connections that runs directly from the app. Then you can set rules how your eBlocker should deal with these connections (activate eBlocker for connections or deactivate your eBlocker for connections). Choose the device on which you are using the app, as well as the duration of the recording, the maximum size of the recording file and start recording afterwards.



Configure manual recording

Record connections for:
Choose device: Dell Inc. (No. 3) (192.168.3.161) (current device)

Stop recording after:
Choose max time: 5 min
Choose max size: 100 MB

HTTPS analysis for selected device

Use the app as usual. Especially test the functions that seem to not be compatible with your eBlocker. Update the list with the recorded connections afterwards.

To find the domains and IP addresses your eBlocker should not be active on, it is necessary to try out different settings. Use the switch slide ("Test temporary rule set"), so the selected rules can be effective temporarily and test the functionalities again.

Please note that the proposed rules may not always be correct, because of some connections that are recorded that do not source from the tested app.

As soon as the app runs smoothly with temporary rules, you can save these rules as a new app definition for good.

8.5 IP-Anon

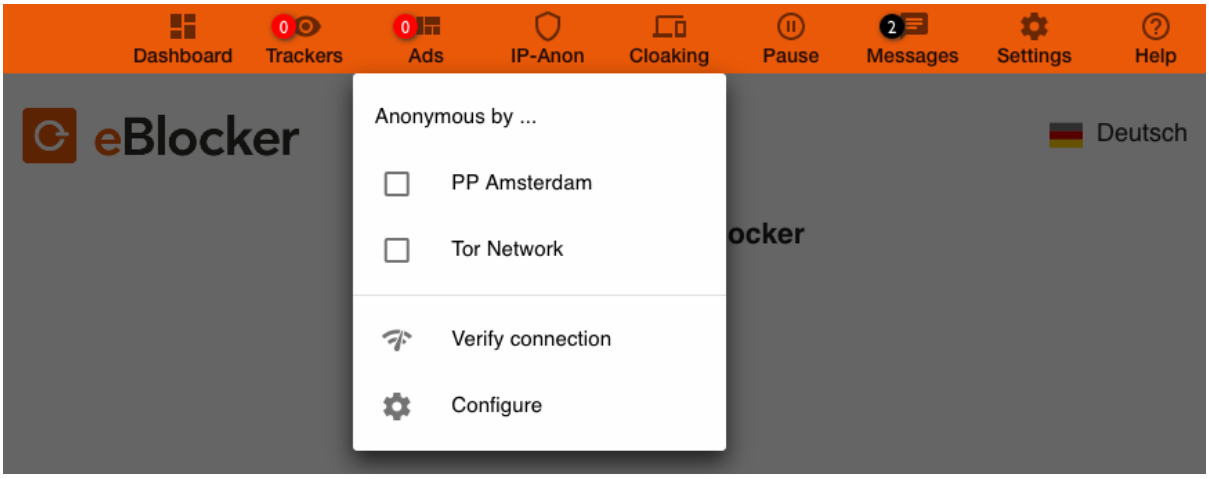
Available for **eBlocker Base**, **eBlocker Pro** and **eBlocker Family**

8.5.1 Setting Up and Using the Tor Network

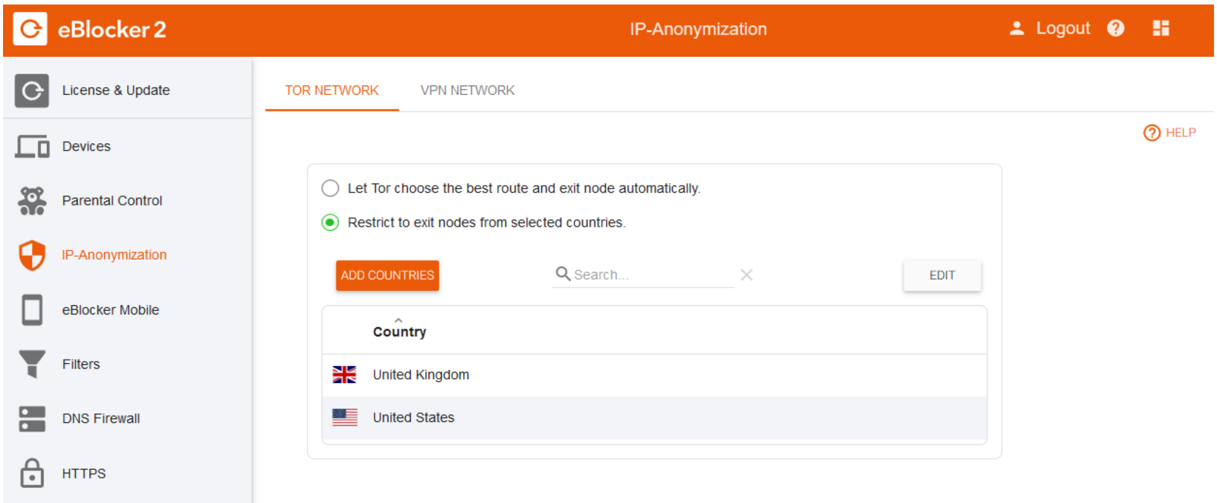
As described in section 7.5, you can disguise your actual IP address by using the anonymization network.

The eBlocker always connects to the IP-Anonymization via the Tor network

To enable the IP anonymization, open the controlbar. Go to “Anon” and click on “Enable IP anonymization”.



On the following page, click on "IP Anonymization" on the left side of the eBlocker console and select the "Tor network" menu item in the upper right corner.

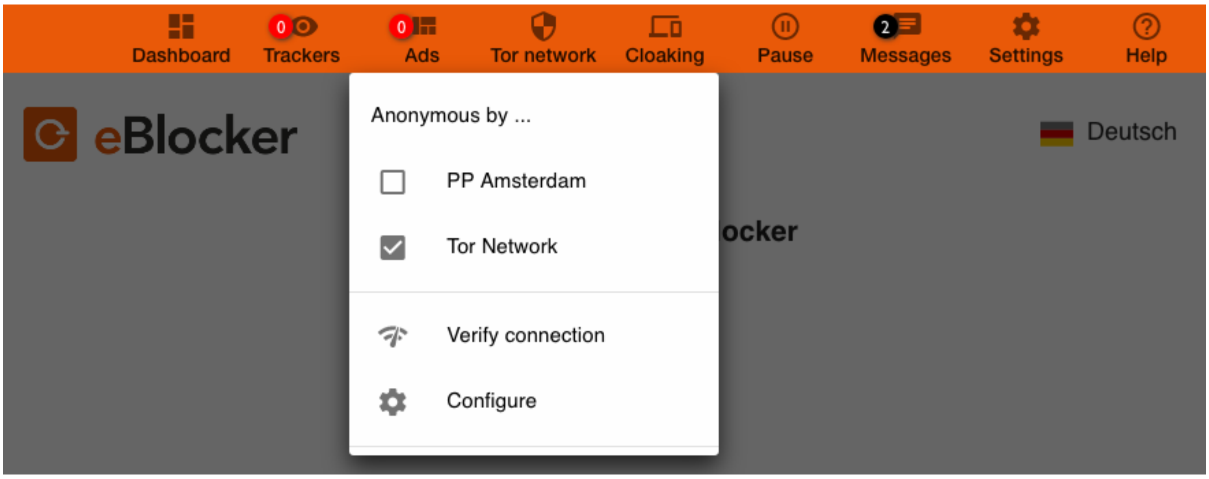


○ Let Tor choose the best route and exit node automatically.

● Restrict to exit nodes from selected countries.

Country
United Kingdom
United States

Click on the button "Add countries". Now you can choose your favorites from the list of countries. Then click on the "Apply" button.



Anonymous by ...

□ PP Amsterdam

☑ Tor Network

Verify connection

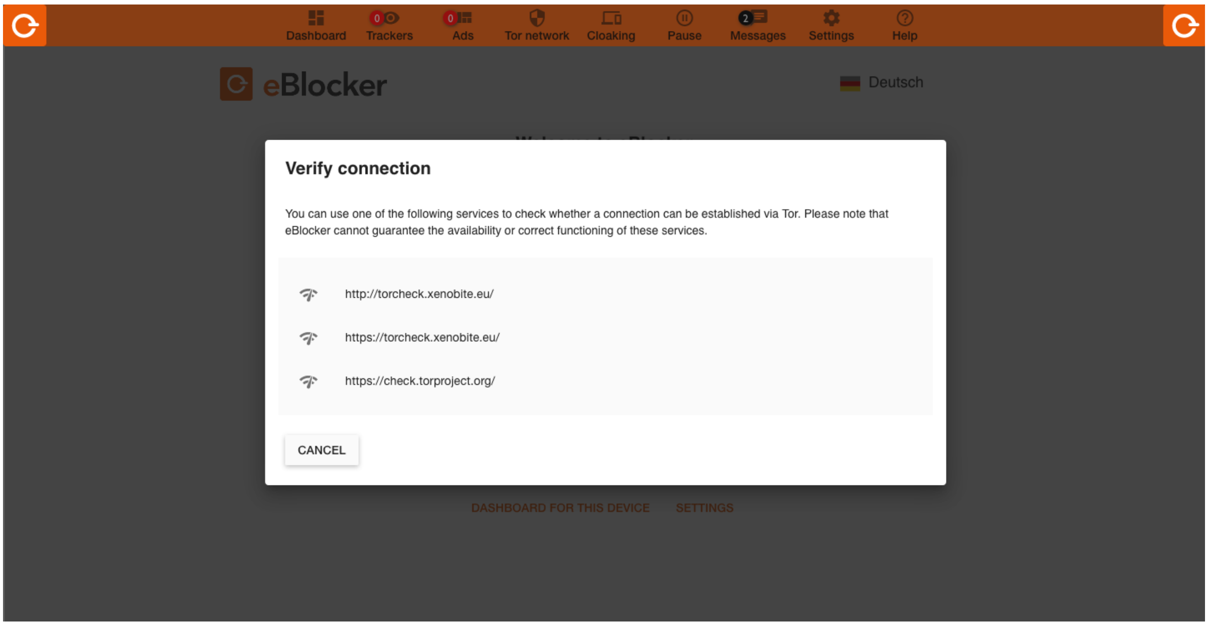
Configure

From now on you can surf anonymously via the IP address assigned to you by the Tor network. An Internet service provider will think that you are located from one of the random chosen countries. Thus you can avoid any censorship or can have access to content that is only available in certain regions of the world.

Please note that the Tor-network is an association of volunteering Internet activists, that provide service cost-free but with no availability guarantee.

If no country is selected, an exit server of a random country will be used.

With a click on "Check connection" you can check if there is a connection to the Tor Network after activating the Tor Network. We have selected three well-known websites for you.



Verify connection

You can use one of the following services to check whether a connection can be established via Tor. Please note that eBlocker cannot guarantee the availability or correct functioning of these services.

http://torcheck.xenobite.eu/

https://torcheck.xenobite.eu/

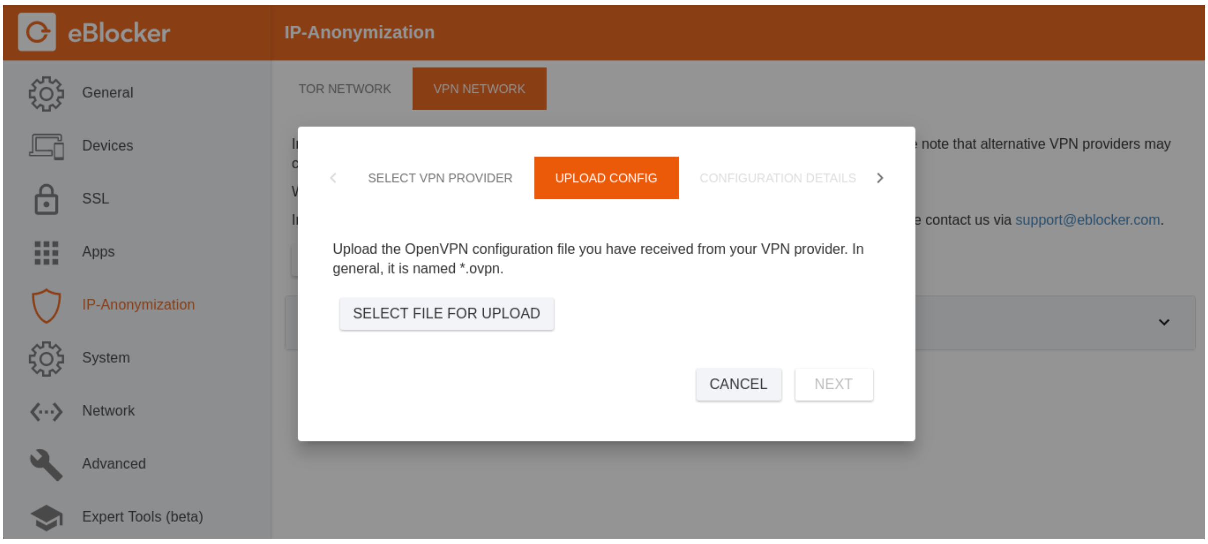
https://check.torproject.org/

By clicking on "Tor: Get new identity" you can switch from the controlbar to another Tor exit server of the country.

To disconnect the Tor connection click on the anon icon first and afterwards on the Tor icon. The checked pattern on the anon icon will then be removed again.

8.5.2 Set up alternative VPN network

Instead of the standard Tor network provided by the eBlocker, you can use a VPN connection from any other VPN provider.
VPN networks can be set up under "eBlocker Settings > IP Anonymization" and "VPN Networks". There, you can also find a link to the list of VPN providers we tested. This list is updated regularly. You can also use other VPN providers as long as they support the OpenVPN protocol.

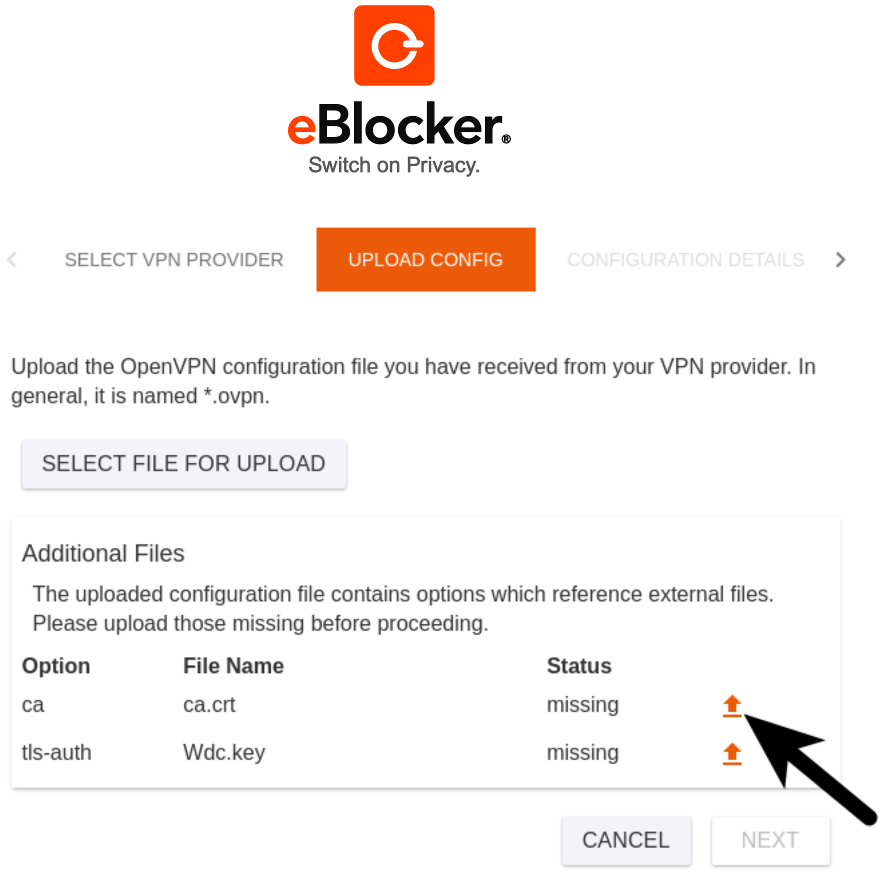


Upload the OpenVPN configuration file you have received from your VPN provider. In general, it is named *.ovpn.

Note:
Other VPN provider may charge additional costs. Connection speed may vary depending on the VPN provider.

Your VPN provider usually provides you with a username, password and a configuration file, it's name ending on the suffix ".ovpn". This configuration file is needed to set up the connection to the VPN network.

To create a new VPN connection, click “New VPN Provider”. Now follow the wizard's instructions and upload the configuration file provided by your VPN provider.



eBlocker
Switch on Privacy.

Upload the OpenVPN configuration file you have received from your VPN provider. In general, it is named *.ovpn.

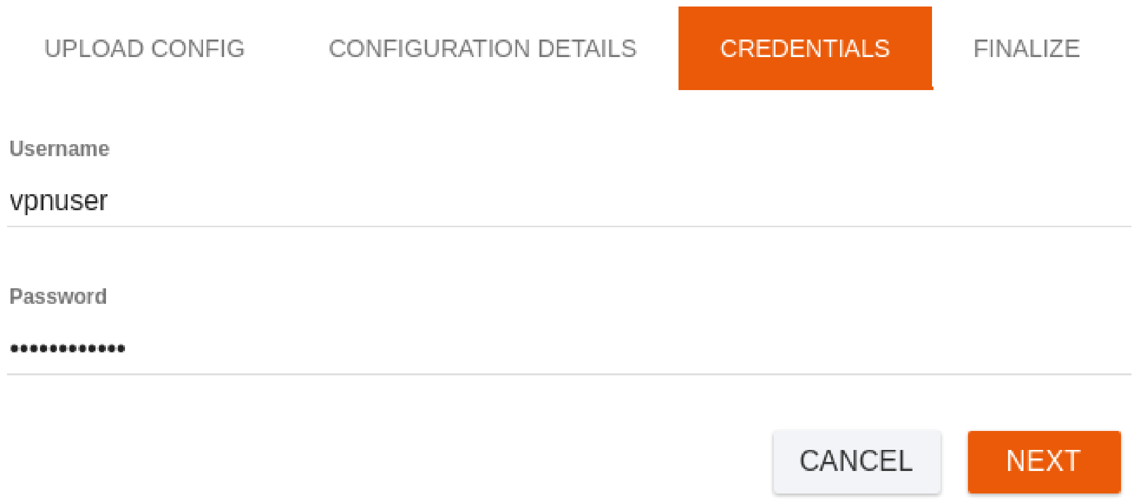
Additional Files

The uploaded configuration file contains options which reference external files. Please upload those missing before proceeding.

Option	File Name	Status
ca	ca.crt	missing
tls-auth	Wdc.key	missing

After uploading the configuration file you have the option to upload other files, if needed. After uploading the files you will be shown details regarding ignored or unsupported options from the eBlocker. This is generally harmless and the ignored or unsupported options will not lead to any kind of malfunction. The eBlocker can still be used optimally. Click on "Next".

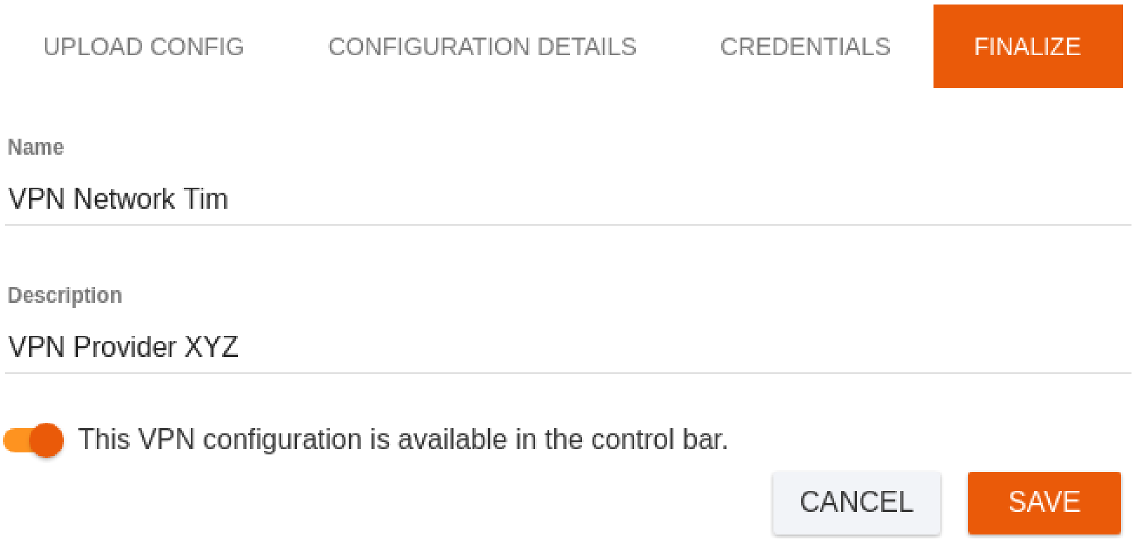
Enter the username and password you have received from your VPN provider into the respective access data fields and click on "Next".



Username
vpnuser

Password
••••••••••••

Enter a name and description for this VPN network. Finally, decide if you wish the VPN network to be available in the eBlocker controlbar by clicking on the switch slide. If you do not want the connection to be shown in the controlbar, it will only be visible in your settings and displayed as inactive.



Name

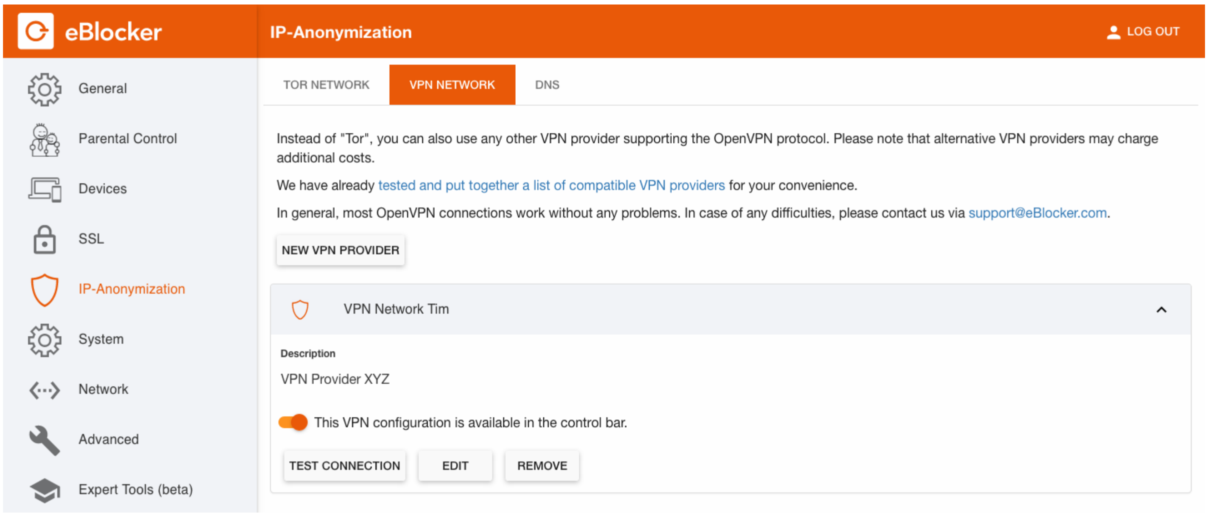
VPN Network Tim

Description

VPN Provider XYZ

This VPN configuration is available in the control bar.

You have successfully created a new VPN network and can edit, remove, or run a connection test with a click on the name.



Instead of "Tor", you can also use any other VPN provider supporting the OpenVPN protocol. Please note that alternative VPN providers may charge additional costs.

We have already tested and put together a list of compatible VPN providers for your convenience.

In general, most OpenVPN connections work without any problems. In case of any difficulties, please contact us via support@eBlocker.com.

VPN Network Tim

Description

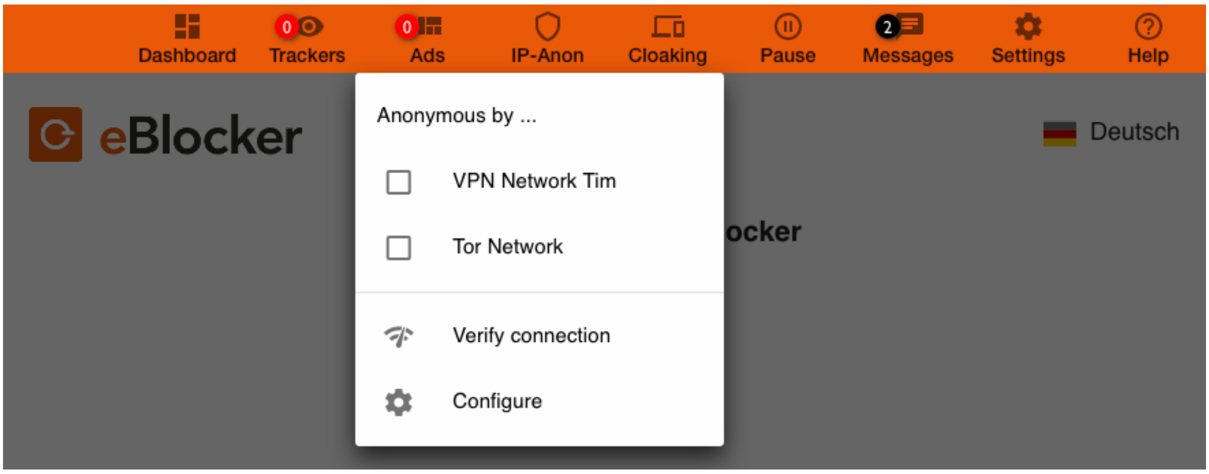
VPN Provider XYZ

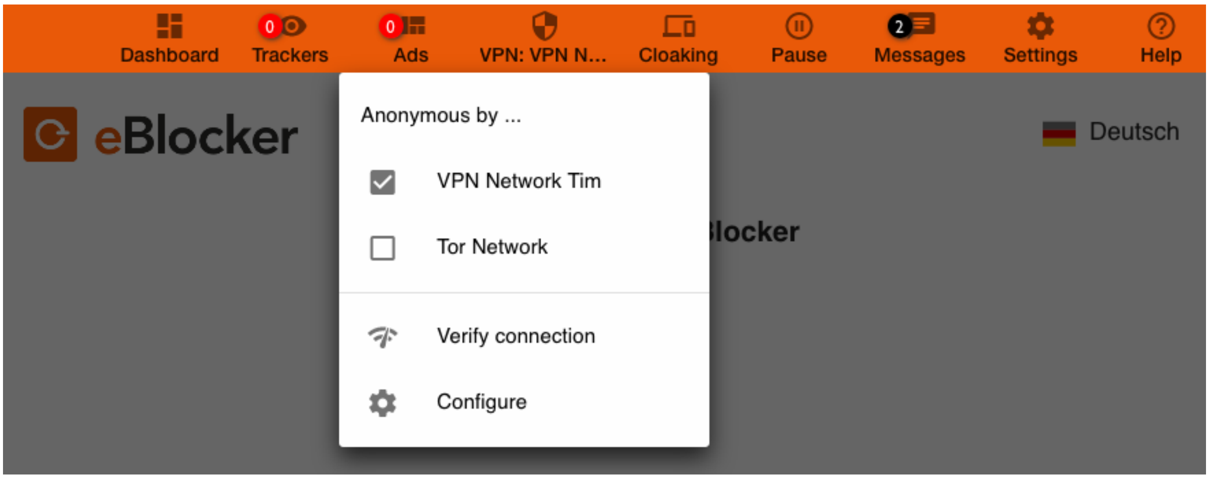
This VPN configuration is available in the control bar.

In the eBlocker Controlbar, you will see the VPN network you have just created under the "Anon" menu item. The connection is verified by clicking on the VPN network, and a check mark is displayed to indicate successful connection to the VPN network. If the connection was not successful, no check mark would be displayed. In this case, go back to settings and verify your username and password.

After activating the VPN network, the Anon icon in the control bar is filled with a checked pattern to indicate it is active.

To disconnect the VPN connection click on the anon icon first and afterwards on the VPN icon. The checked pattern on the anon icon will then be removed again.



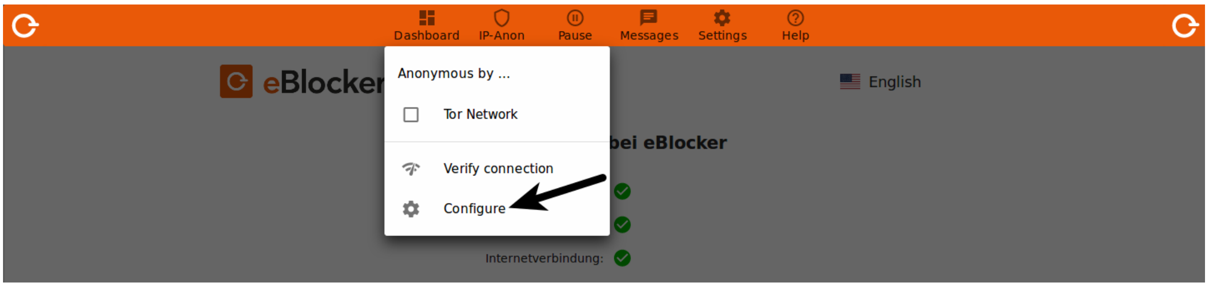


To disconnect, first click the Anon icon and then the VPN network. The Anon icon in the control bar will be empty and the eBlocker will automatically be connected to *Tor*.

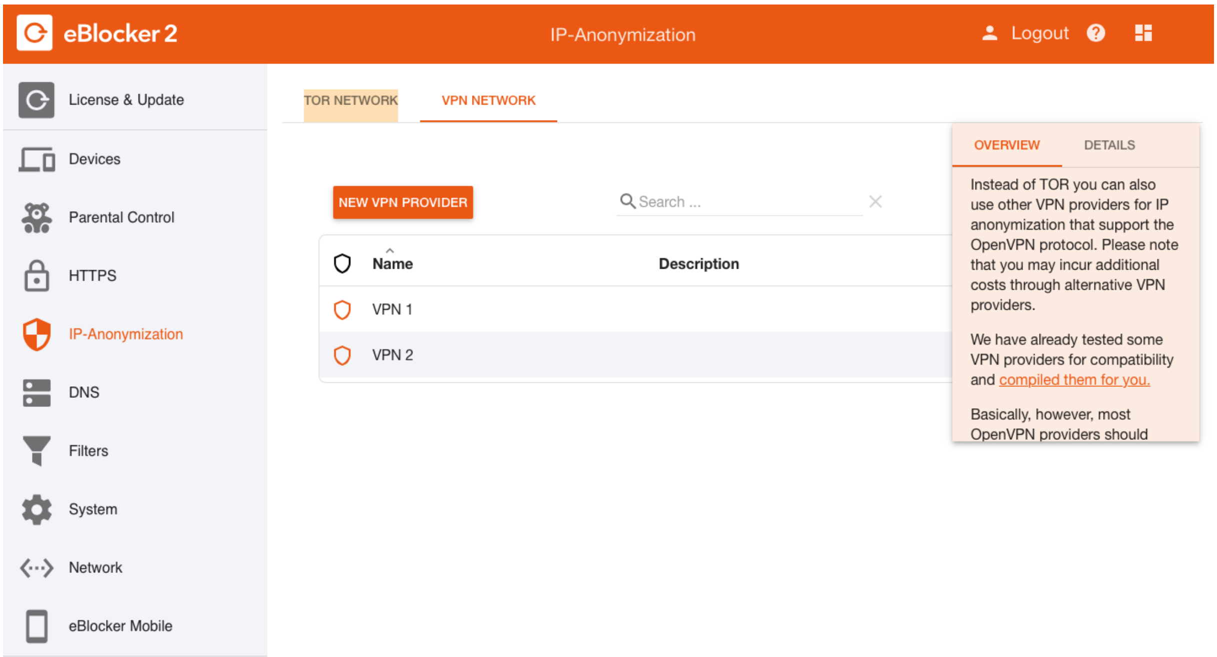
Note:
A Tor connection cannot be used simultaneously with an existing VPN or another existing Tor connection.

8.5.3 Set up the VPN-network from Perfecty Privacy

Click the eBlocker icon and open the eBlocker controlbar. With a click on „IP-Anon“, a pulldown menu opens. Go to “configure”.



A new site opens. Click on the tab „VPN-Network“ and then go to „Overview“, where a drop out opens. You can then click on the VPN provider compatibility list that we have complief for you.



eBlocker 2 | IP-Anonymization | Logout

- License & Update
- Devices
- Parental Control
- HTTPS
- IP-Anonymization
- DNS
- Filters
- System
- Network
- eBlocker Mobile

TOR NETWORK | VPN NETWORK

NEW VPN PROVIDER | Search ...

Name	Description
VPN 1	
VPN 2	

OVERVIEW | DETAILS

Instead of TOR you can also use other VPN providers for IP anonymization that support the OpenVPN protocol. Please note that you may incur additional costs through alternative VPN providers.

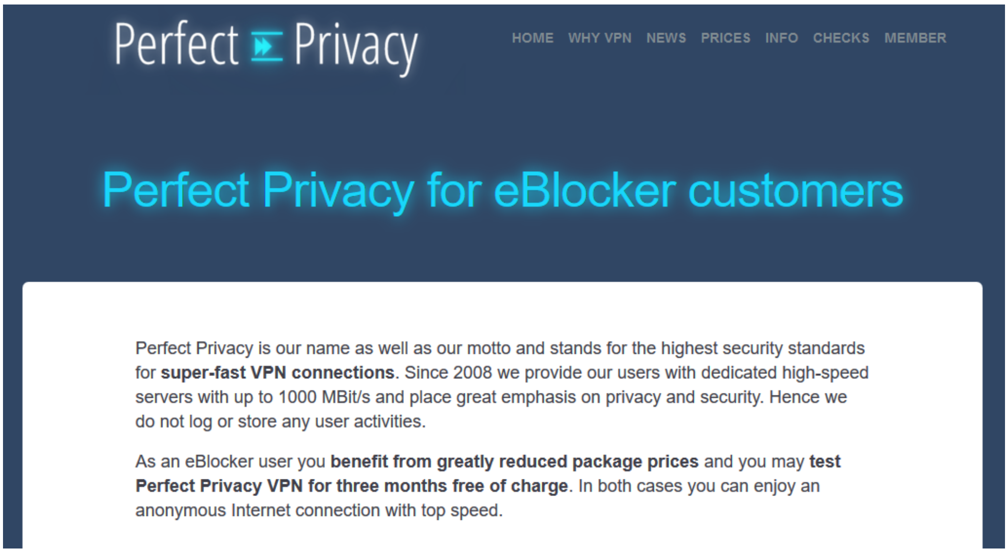
We have already tested some VPN providers for compatibility and compiled them for you.

Basically, however, most OpenVPN providers should

You are now lead to a site where all VPN networks are listed that have been tested by us. Click on “Perfect Privacy”.

Perfect Privacy
Test 3 Months For Free*

You are now visiting the website of Perfect Privacy.

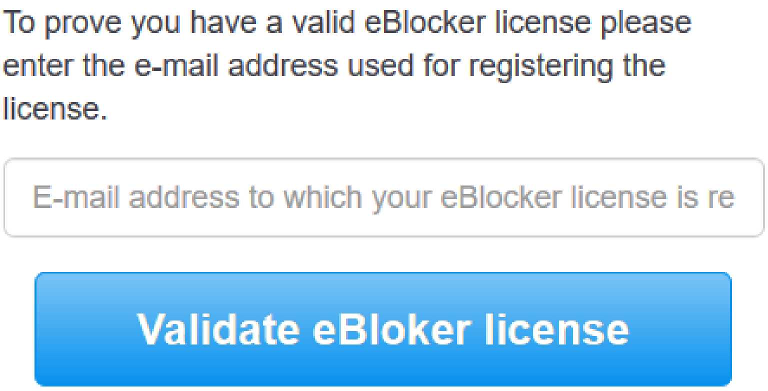


Perfect Privacy for eBlocker customers

Perfect Privacy is our name as well as our motto and stands for the highest security standards for **super-fast VPN connections**. Since 2008 we provide our users with dedicated high-speed servers with up to 1000 MBit/s and place great emphasis on privacy and security. Hence we do not log or store any user activities.

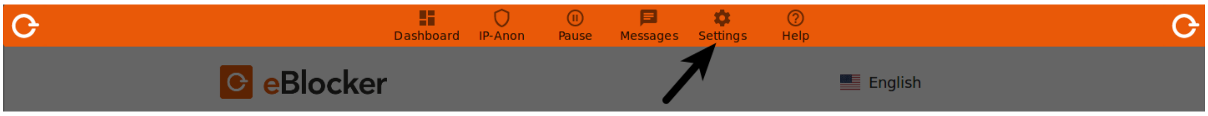
As an eBlocker user you **benefit from greatly reduced package prices** and you may **test Perfect Privacy VPN for three months free of charge**. In both cases you can enjoy an anonymous Internet connection with top speed.

Scroll down to the bottom. Type-in the exact same email address with which you have registered your eBlocker with. Click on the blue area „eBlocker Lizenz prüfen“.


To prove you have a valid eBlocker license please enter the e-mail address used for registering the license.

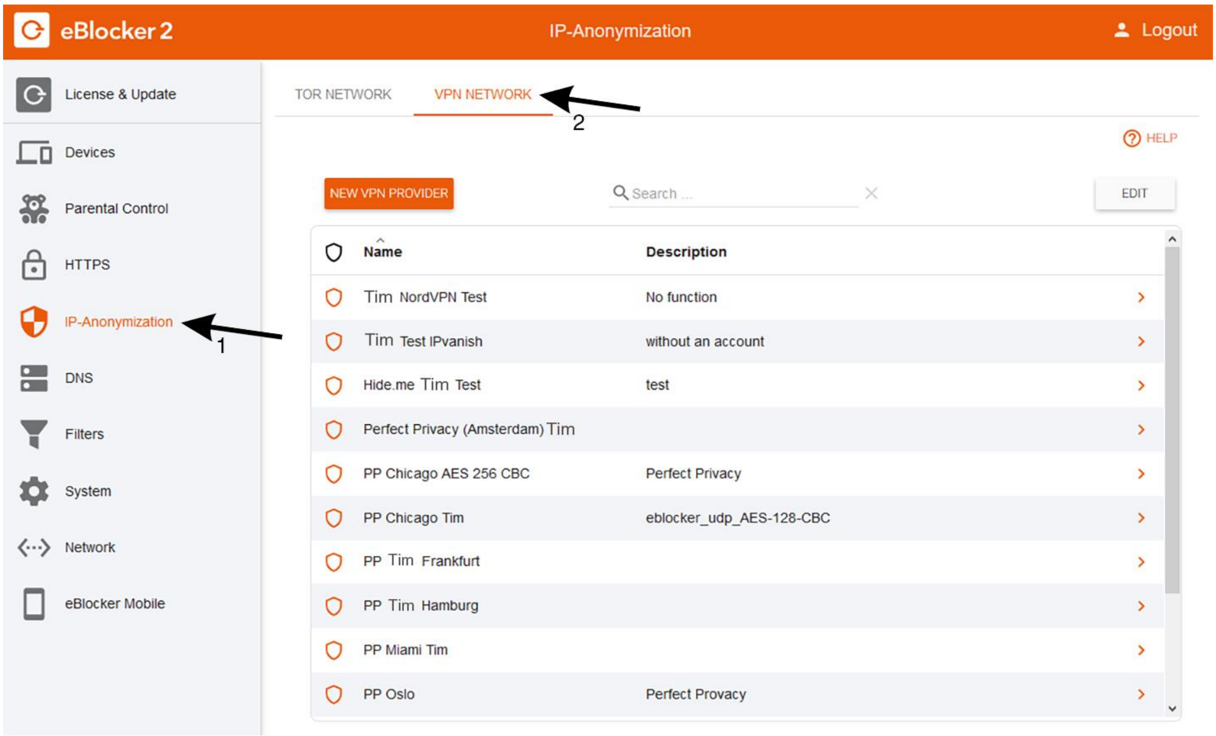
A username, a password and e configuration file with the ending „.ovpn“ is now provided by your VPN provider. This configuration file is necessary to setup the VPN network connection. Download the configuration file and make a note where you have saved the file so you can easily locate it again.

Open the eBlocker controlbar and click on „Settings“.



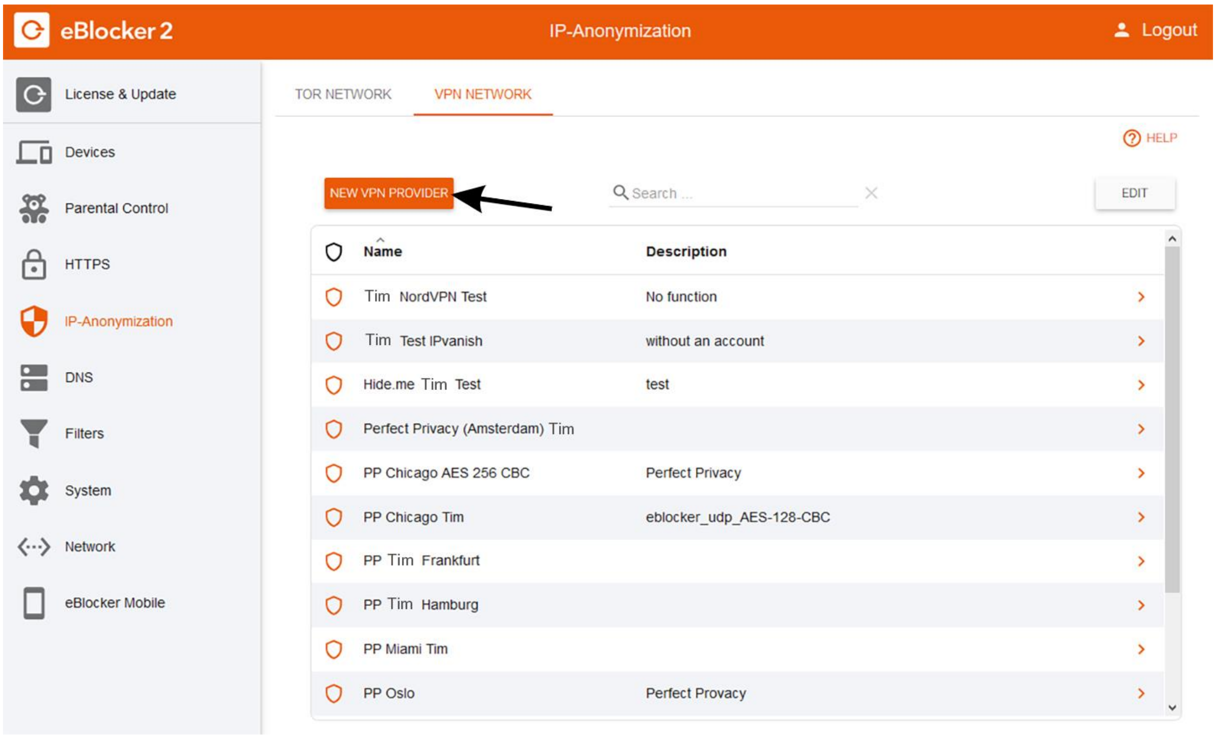
Click on „IP-Anonymization“ on the following site that appears.

The content changes on the right side. Click on „VPN Network“.



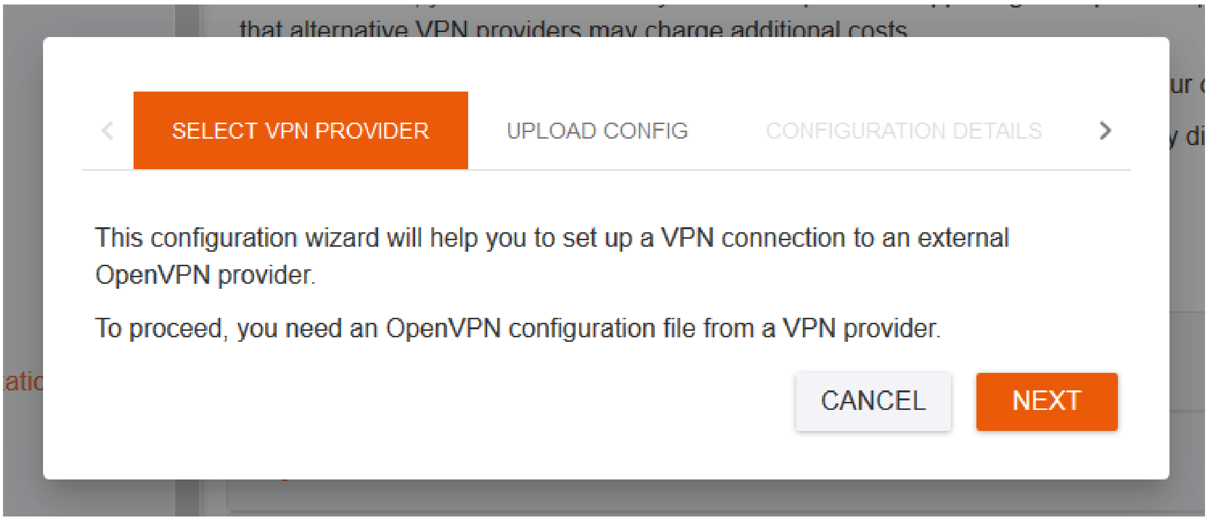
Name	Description
Tim NordVPN Test	No function
Tim Test IPvanish	without an account
Hide.me Tim Test	test
Perfect Privacy (Amsterdam) Tim	
PP Chicago AES 256 CBC	Perfect Privacy
PP Chicago Tim	eblocker_udp_AES-128-CBC
PP Tim Frankfurt	
PP Tim Hamburg	
PP Miami Tim	
PP Oslo	Perfect Provacy

Now click on the button „New VPN provider“.



Name	Description
Tim NordVPN Test	No function
Tim Test IPvanish	without an account
Hide.me Tim Test	test
Perfect Privacy (Amsterdam) Tim	
PP Chicago AES 256 CBC	Perfect Privacy
PP Chicago Tim	eblocker_udp_AES-128-CBC
PP Tim Frankfurt	
PP Tim Hamburg	
PP Miami Tim	
PP Oslo	Perfect Provacy

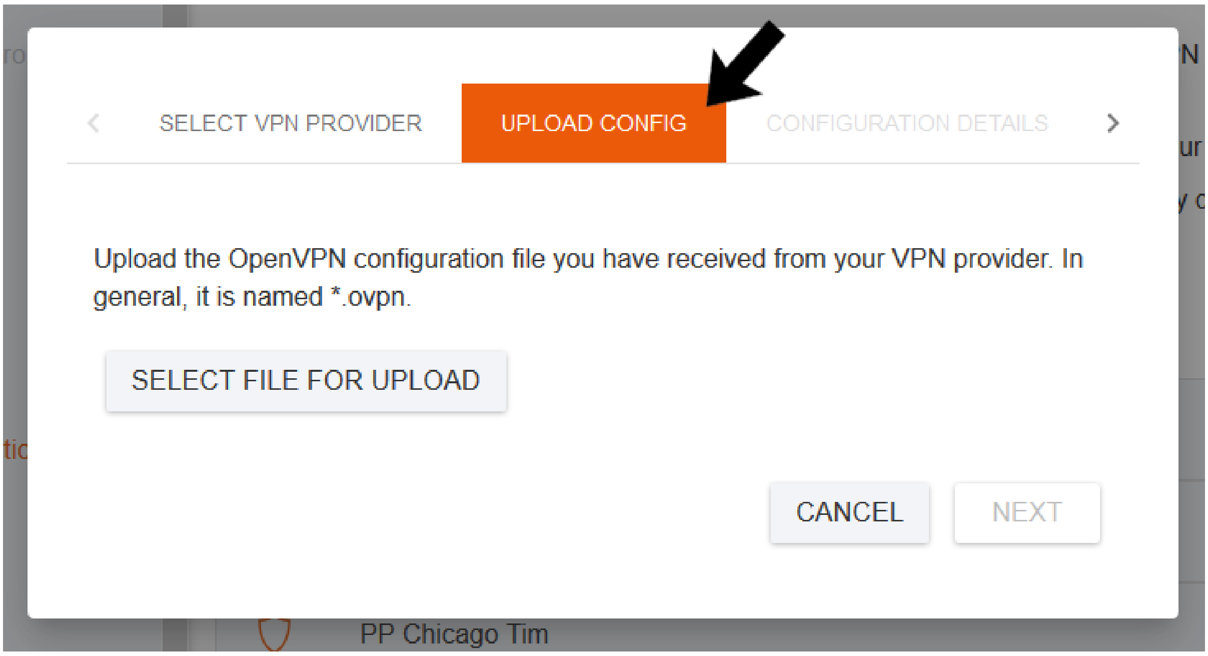
A popup window opens. This wizard supports you with setting up VPN.



This configuration wizard will help you to set up a VPN connection to an external OpenVPN provider.

To proceed, you need an OpenVPN configuration file from a VPN provider.

Click on „Upload configuration“ and upload your file.



Upload the OpenVPN configuration file you have received from your VPN provider. In general, it is named *.ovpn.

After uploading the configuration file you may have the opportunity to upload more files. You will receive more information afterwards. The information contains not supported options by the eBlocker for e.g., that are usually harmless and are not marked as error. The eBlocker can be further used with no problems. Click on “weiter”.

Type-in your username and password that you have received from your VPN provider in the section „Zugangsdaten“. Click on „Weiter".

Assign a name and description fort he VPN network. Decide if the VPN network should be available in the controlbar.

Finish the process with „Abschließen“. You are now surfing anonymous via the VPN network of Perfect Privacy and have saved a **3 months cost free service of VPN**.

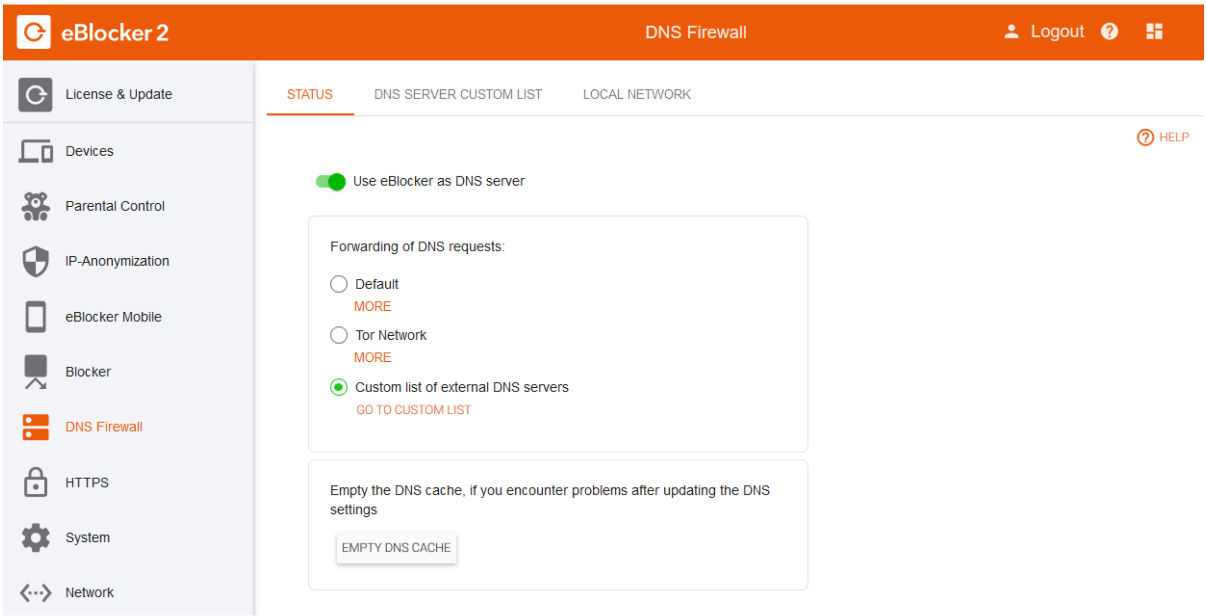
The VPN network which you have just setup is now visible below the “Anon”. By clicking on the VPN network, the connection is tested first.
The successful connection to the VPN network is displayed with a tick mark. If the connection has not been successful, no tick mark will be displayed. If the connections was not successful, go back to your settings and check your username and password.

The VPN service can be individually enabled for every device.

8.6 DNS

If you enable this feature, you can use your eBlocker to distribute DNS requests to a list of different DNS servers or have them resolved over the Tor network. There are three different options available to you.

- Default
- Tor-Network
- Custom list of external DNS servers



Use eBlocker as DNS server

Forwarding of DNS requests:

○ Default
MORE

○ Tor Network
MORE

● Custom list of external DNS servers
GO TO CUSTOM LIST

Empty the DNS cache, if you encounter problems after updating the DNS settings

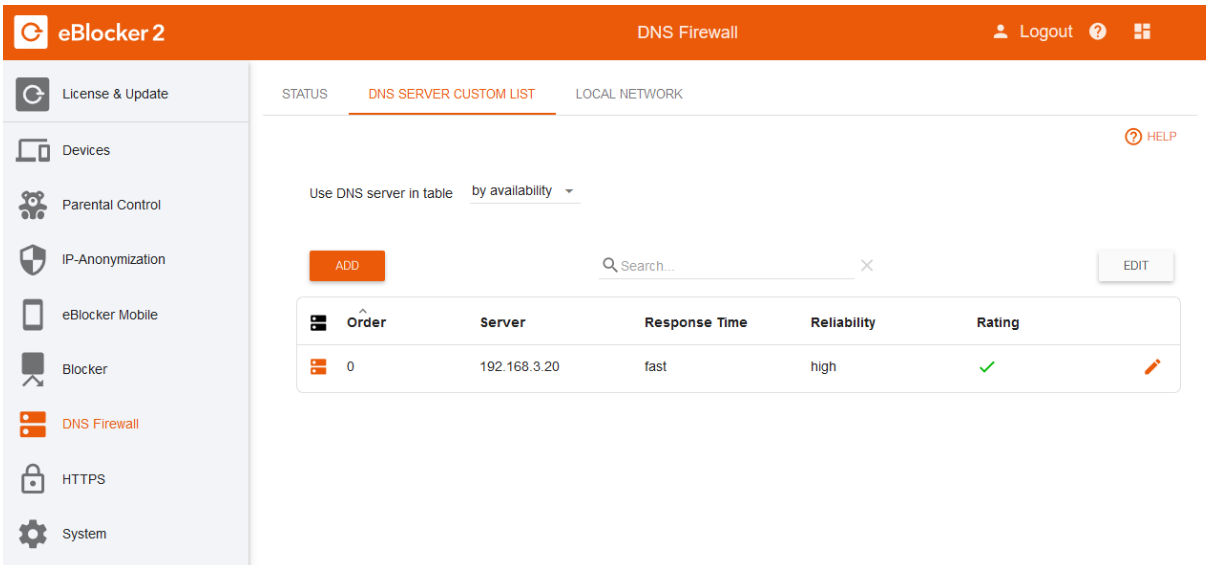
EMPTY DNS CACHE

Internet Provider
The setting of your local network is used here. This means that the DNS server is used, which you have stored in your router configuration.

Tor-Network
Here, the DNS requests are routed through the Tor network and passed to a DNS server at the Tor network starting point. Make sure Tor is available. You can check this in the IP Anonymization > Tor Network menu.
The DNS function should not currently be used if you operate your own DNS server in the local network. Otherwise, problems may occur when resolving internal or external IP addresses.

Custom list of external DNS servers

With this option you can store a list of DNS servers. This list can then be processed by the eBlocker in order of availability or in random order. You can create the individual DNS servers in the "DNS Server List" tab.



Use DNS server in table by availability

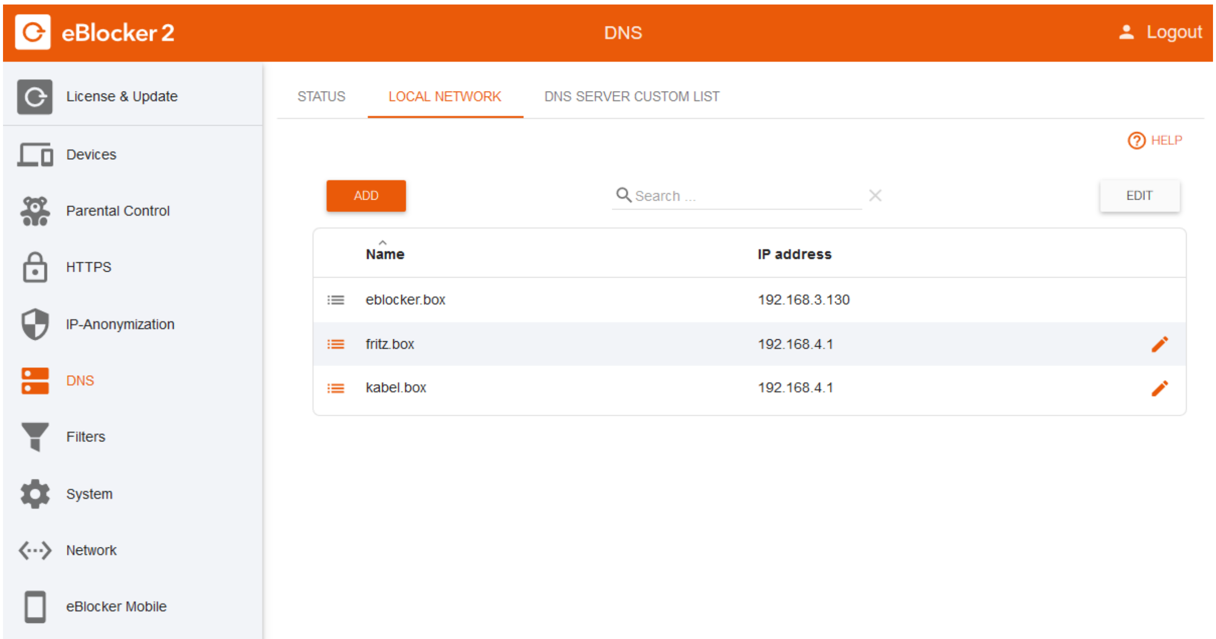
Order	Server	Response Time	Reliability	Rating
0	192.168.3.20	fast	high	✓

8.6.1 DNS – Local Device names

Here you can assign a server name to specific IP addresses for your network.

Example: If you use a Fritzbox, you will have noticed that you can no longer call fritz.box in your browser when the eBlocker DNS function is activated. This is because the DNS server is used by the eBlocker and no longer by the Fritzbox. The eBlocker does not recognize the fritz.box.

Click on the button "Add" and assign a server name such as fritz.box. Now enter the IP address of your Fritzbox in the IP address field (example: 192.168.178.1). Now click on the button "Save" and you will see a new entry in the list.



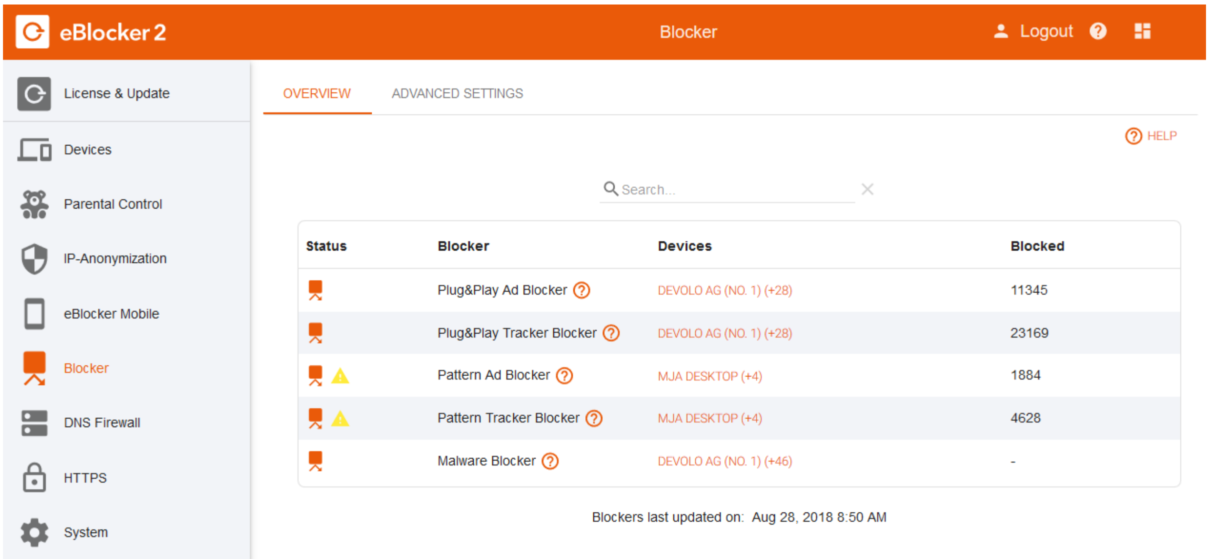
Name	IP address
eblocker.box	192.168.3.130
fritz.box	192.168.4.1
kabel.box	192.168.4.1

If you now enter fritz.box in a browser, you should reach the settings of your Fritzbox again.

8.7 Blocker

8.7.1 Blocker – Overview

Here you get an overview of the used blocker features of the eBlocker. If you move the mouse over the individual symbols, you will receive further information.



Status	Blocker	Devices	Blocked
	Plug&Play Ad Blocker ?	DEVOLO AG (NO. 1) (+28)	11345
	Plug&Play Tracker Blocker ?	DEVOLO AG (NO. 1) (+28)	23169
⚠	Pattern Ad Blocker ?	MJA DESKTOP (+4)	1884
⚠	Pattern Tracker Blocker ?	MJA DESKTOP (+4)	4628
	Malware Blocker ?	DEVOLO AG (NO. 1) (+46)	-

Blockers last updated on: Aug 28, 2018 8:50 AM

Status

Move your mouse over the status icon and you will get a short information about the filter and the number of devices using this blocker.

If you see a yellow triangle behind the status symbol, this is an extra reference to the blocker. If you move the mouse over the yellow triangle, the note is displayed.

Blocker

There are three blocker features.

- The domain blockers for ads and trackers block advs and trackers as soon as the domain is accessed. This blocker can also be used without activating the eBlocker SSL feature.
- The Pattern Blockers for Ads and Tracker recognize the trackers and ads based on patterns. For these blockers the activation of the eBlocker SSL feature is necessary.
- Malware and Phishing Blockers

Devices

Here you can see a list of all devices that currently use this blocker. If you move the mouse over the devices, a list of all devices is displayed.

Blocked Requests

Here you see a list of all blocked requests from all devices since the start of your eBlocker.

8.7.2 Blocker – Advanced Features

Available for **eBlocker Pro** and **eBlocker Family**

Captive Portal Check

Google Captive Portal Check is used by Google products such as Android, Chrome and Chromebooks to test whether an Internet connection exists. Your IP address is sent to the Google Captive Portal. eBlocker blocks the structure of the Google Captive Portal, otherwise Google will collect your IP address. Activate this option with one click if Android devices are often disconnected from your WLAN.

Do Not Track

Do-Not-Track (DNT) is an HTTP header field which signals to a website that the visitor does not want a user profile to be created from the website. Unfortunately, this wish of the user is not binding and is therefore ignored by many websites.

For most browsers, this feature can be found in the privacy or security settings.

The eBlocker makes it easier for you and automatically sets the Do-Not-Track field in all requests after activation of the function.

HTTP Referrer Header

HTTP referrer headers are automatically created when you surf the Internet. The referrer displays the website you visited before you reached the current website.

By using the referrer headers, websites can partially track your surfing habits. Some websites also use the referrer headers for internal purposes. Blocking the referrer headers can therefore result in some pages no longer being displayed correctly. Decide with one click whether referrer headers should be allowed.

Compression

Web servers often compress the delivered web pages in order to keep the amount of data transferred on the Internet as low as possible. The eBlocker must then decompress the data to analyze the page and perform its protection features. In your local network, re-compressing on the last track to the device would not result in a speed advantage. On the contrary: The page layout is usually even faster if no new compression and decompression is used for this last track.

Only if your device is connected via eBlocker Mobile while on the go it should be compressed to the device.

Therefore the compression feature of the eBlocker offers you three settings.

No Compression

The data between eBlocker and device is not compressed again.

Compression for eBlocker Mobile Devices (recommended)

As above. Only if your device connects via eBlocker Mobile while on the go, the data between eBlocker and device will be compressed

Always compress

Here the data is always compressed during transport from the eBlocker to the device.

WebRTC

WebRTC is a browser technology that enables real-time communication between two parties. It is used, for example, for Internet telephony and chat.

Unfortunately, WebRTC reveals your real IP address (and even your local LAN IP) to establish the connections. Even when using Tor (IP anonymization), you can be identified by your real IP address if WebRTC is not blocked. Decide with one click whether WebRTC connections should be allowed.

8.8 System

Available for **eBlocker Base**, **eBlocker Pro** and **eBlocker Family**

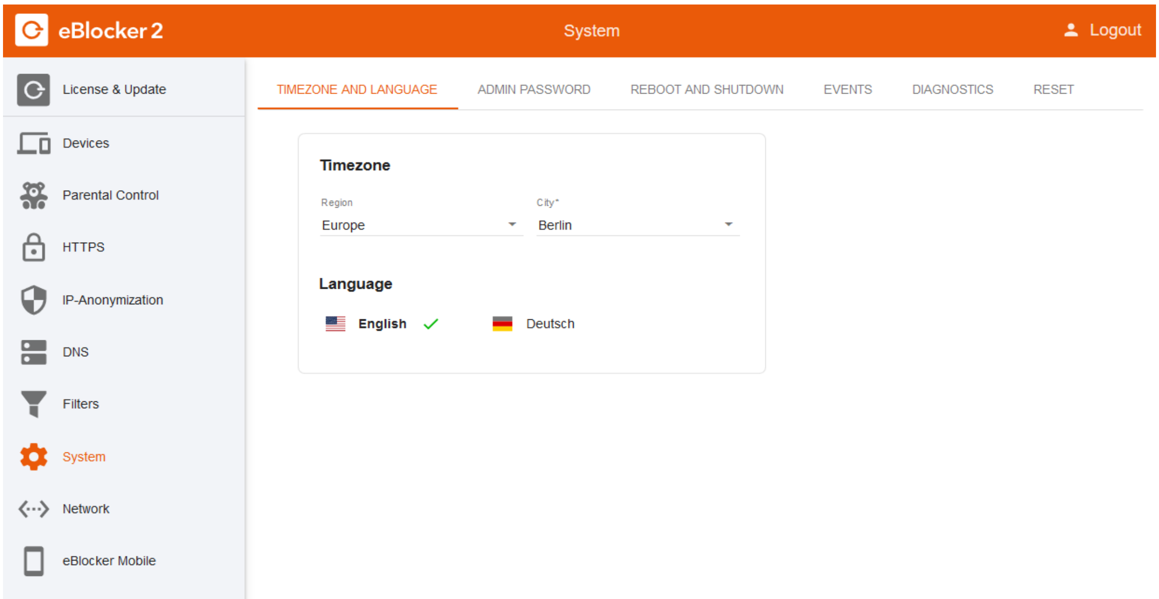
By clicking on „System“ you can apply following settings:

8.8.1 System – Language and time zone

Set the time zone and language of the eBlocker Controlbar and eBlocker Console.

To set the time zone, first select the region and then the city of your country.

To set the language, click either English or German. The desired language is changed immediately.



Timezone

Region: Europe

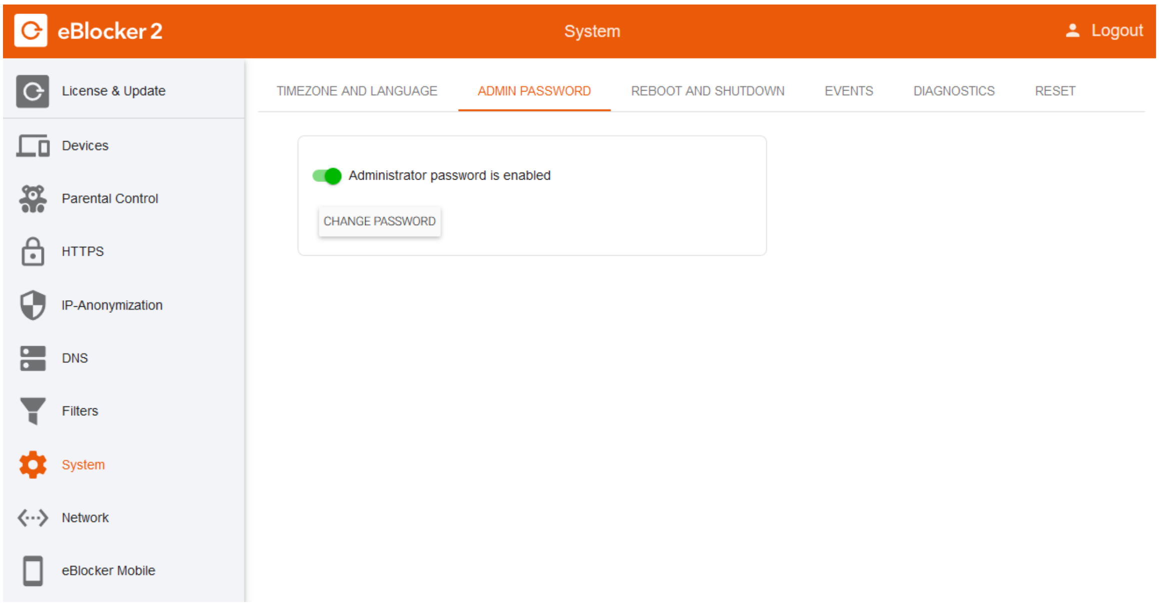
City*: Berlin

Language

English ✓ Deutsch

8.8.2 System - Admin-Password

Activate the admin password for your eBlocker. You can also change the current admin password here.



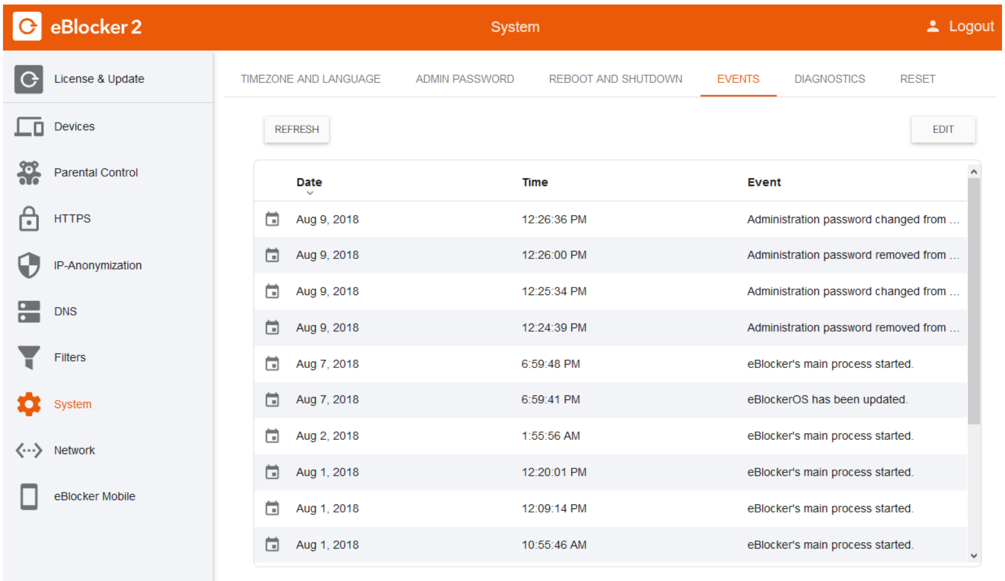
Administrator password is enabled

8.8.3 System - Reboot and Shutdown

From this page you can restart or shut down eBlocker.
To restart eBlocker after shutting it down, unplug the device, wait 30 seconds and then reconnect it to the power supply.

8.8.4 System - Events

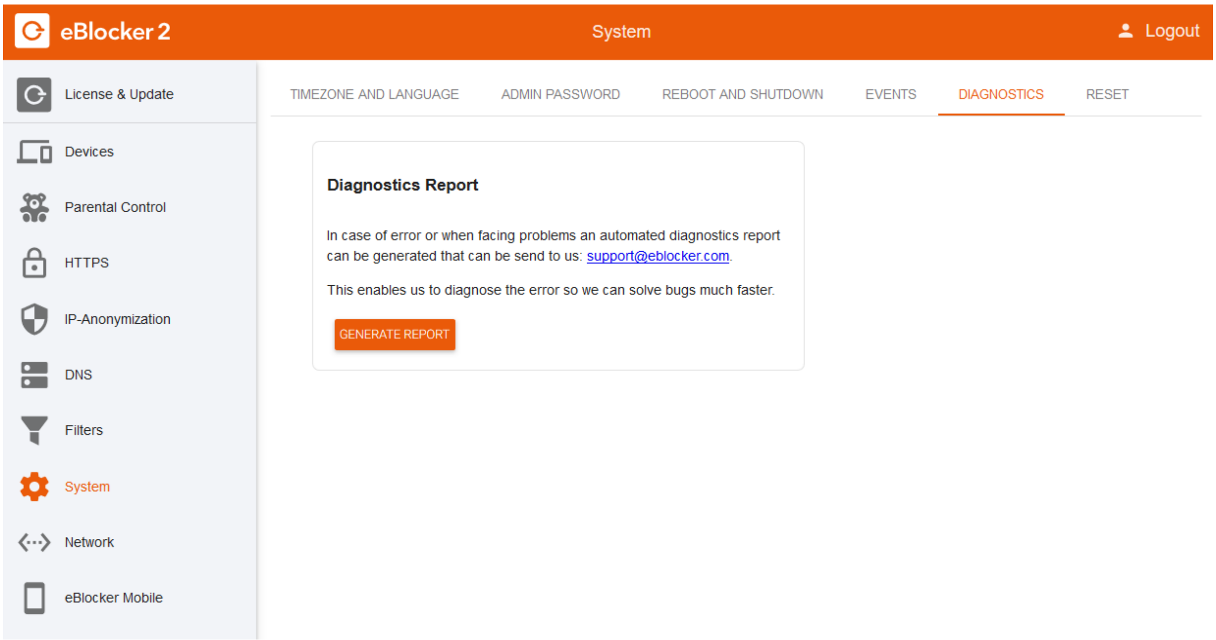
The eBlocker detects events such as the network connection being disconnected or the power supply being disconnected without shutting down the eBlocker. Such events are recorded here for your information. You are notified in the control bar if there is a new entry in the event list.



Date	Time	Event
Aug 9, 2018	12:26:36 PM	Administration password changed from ...
Aug 9, 2018	12:26:00 PM	Administration password removed from ...
Aug 9, 2018	12:25:34 PM	Administration password changed from ...
Aug 9, 2018	12:24:39 PM	Administration password removed from ...
Aug 7, 2018	6:59:48 PM	eBlocker's main process started.
Aug 7, 2018	6:59:41 PM	eBlockerOS has been updated.
Aug 2, 2018	1:55:56 AM	eBlocker's main process started.
Aug 1, 2018	12:20:01 PM	eBlocker's main process started.
Aug 1, 2018	12:09:14 PM	eBlocker's main process started.
Aug 1, 2018	10:55:46 AM	eBlocker's main process started.

8.8.5 System - Diagnostics report

If an error occurs, you can generate an automatic diagnostic report via this page, which you can send to us at the e-mail address support@eblocker.com This allows us to find a faster solution. Simply create the diagnostic report by clicking on the orange "Generate diagnostic report" button and wait a few seconds. Afterwards you have the possibility to download the file and send it to our support. We will contact you as soon as possible.



Diagnostics Report

In case of error or when facing problems an automated diagnostics report can be generated that can be send to us: support@eblocker.com.

This enables us to diagnose the error so we can solve bugs much faster.

8.8.6 System – Reset

Save Settings

Here you have the possibility to save some of your settings. If necessary, you can create a backup before restoring the eBlocker factory settings and restore it after restoring the factory settings.

If you click on the "Save settings" button, the following data is saved in a backup file.

- Trusted Apps
- Trustworthy websites

The backup file is saved in your download directory.

To restore a backup file, simply click on the "Restore settings" button and select the backup file from your download directory.

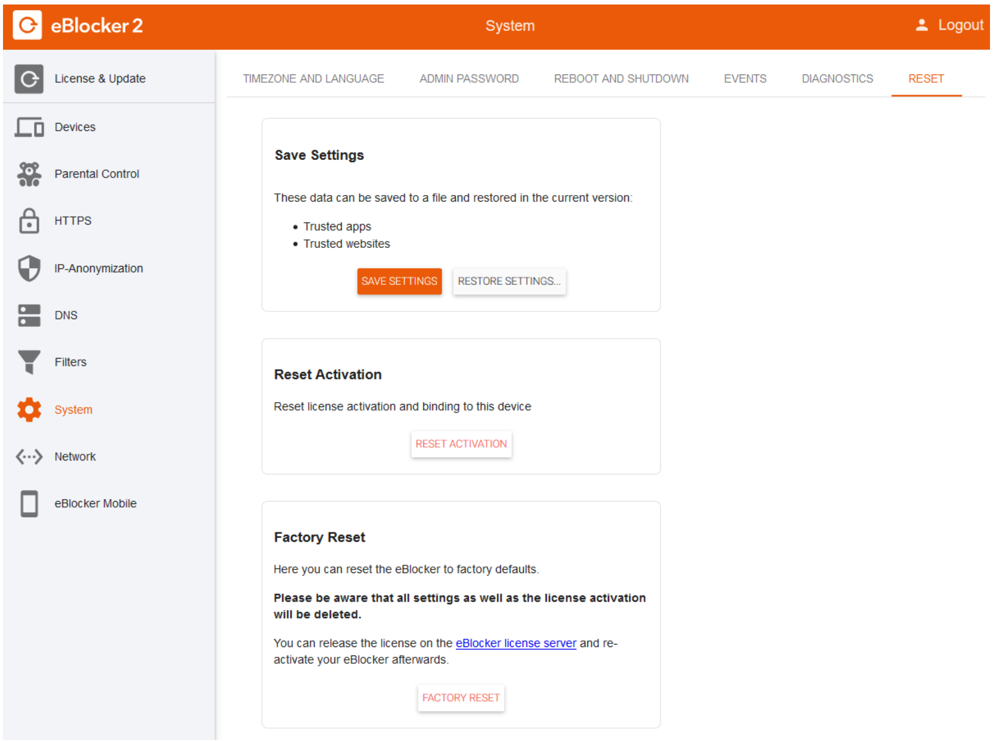
Reset Activation

To reset the activation and license binding of the device, click on "Reset activation". A new window will appear asking if you really want to remove the license from the device. If you want to remove the license, please enter the e-mail address you used when activating the device. Please note that this process cannot be undone.

Factory Settings

Here you can reset the eBlocker to the factory settings. Please note that all settings and activation will be deleted.

You can reset the license via the eBlocker license server and then reactivate your eBlocker. Please go to the website https://www.eblocker.com/en/license-transfer/ and enter the email address with which you activated the eBlocker license. Afterwards you will receive an email from our license server and only need to follow the instructions of this email.



Save Settings

These data can be saved to a file and restored in the current version:

- Trusted apps
- Trusted websites

Reset Activation

Reset license activation and binding to this device

Factory Reset

Here you can reset the eBlocker to factory defaults.

Please be aware that all settings as well as the license activation will be deleted.

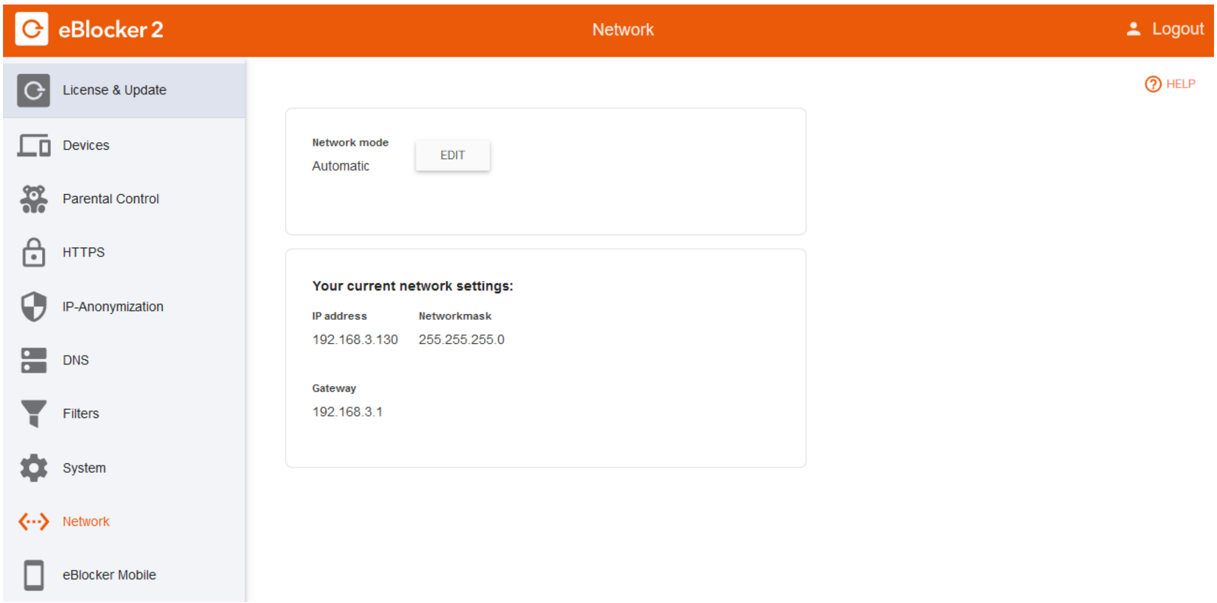
You can release the license on the eBlocker license server and re-activate your eBlocker afterwards.

8.9 Network

Available for **eBlocker Base**, **eBlocker Pro** and **eBlocker Family**

In most of all cases your eBlocker can be configured in the automatic configuration mode.

In some cases, for example if you have a special networking infrastructure, you might have to setup your eBlocker individually so you can use your device optimally.



Network mode
Automatic

Your current network settings:

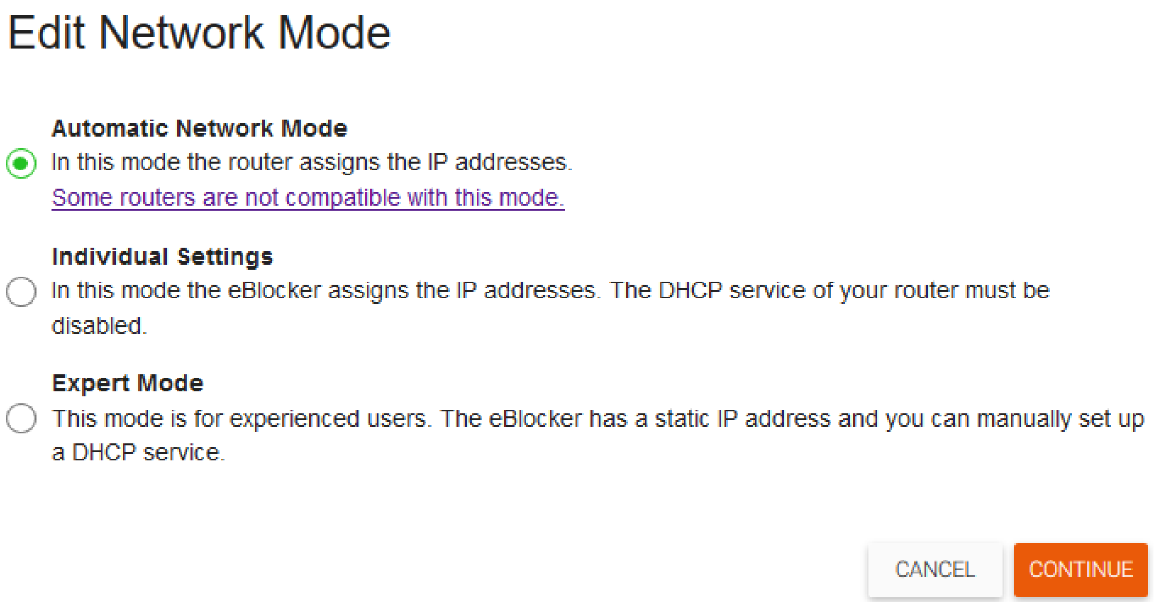
IP address
192.168.3.130

Networkmask
255.255.255.0

Gateway
192.168.3.1

In some cases, for example if you have a special network infrastructure, it may be necessary to change the network configuration of the eBlocker in order to make optimum use of the eBlocker.

The eBlocker offers three different network modes:



Edit Network Mode

● **Automatic Network Mode**
In this mode the router assigns the IP addresses.
Some routers are not compatible with this mode.

○ **Individual Settings**
In this mode the eBlocker assigns the IP addresses. The DHCP service of your router must be disabled.

○ **Expert Mode**
This mode is for experienced users. The eBlocker has a static IP address and you can manually set up a DHCP service.

Automatic network mode

In this mode your router assigns the IP addresses in your network with its DHCP service. The eBlocker is compatible with most routers, but there are a few routers that can't work with the eBlocker like this.

Individual Settings

In this mode the eBlocker assigns the IP addresses in the network. To do this, the DHCP service of the router must be switched off. The eBlocker then takes over the tasks of the DHCP service in your network. Almost all routers are compatible with eBlocker in this mode. You will be accompanied through the setup of the "individual settings" by an assistant, which will give you step-by-step assistance.

Expert mode

In this mode, experienced users can edit the network settings of the eBlocker. These settings make sense, for example, if you operate your own DHCP server in your network.

8.10 eBlocker Mobile

eBlocker Mobile is based on OpenVPN. Your eBlocker becomes a VPN server to which you can connect from a mobile device. Once connected to the eBlocker via OpenVPN, you surf mobile with exactly the same protection you're used to at home. This requires the installation of an OpenVPN client for your mobile device and the installation of the corresponding eBlocker VPN configuration file. As soon as you activate the eBlocker Mobile feature, an assistant will help you setting up the mobile feature. You need an App for your operating system, that opens a VPN Tunnel to your home network.

Download and install a free OpenVPN app, get the config file from your eBlocker dashboard and establish the connection:

OpenVPN Clients for macOS

Tunnelblick (Open Source GNU General Public License)

Tunnelblick
OpenVPN for Mac OS X

OpenVPN Clients for iOS

OpenVPN Connect for iPhone

Download on the App Store

OpenVPN Connect for iPad

Download on the App Store

OpenVPN Clients for Android

OpenVPN Connect

GET IT ON Google Play

After you have successfully installed an OpenVPN app for your operating system, the eBlocker Mobile configuration file must now be loaded and added to the OpenVPN app.

All steps must be performed on the device for which you want protection by your eBlocker while on the move! You must be connected to your home network during installation.

Android

- Download the OpenVPN configuration file for this device in the eBlocker Dashboard (Download Button on the eBlocker Mobile Card)
- Confirm “Open in OpenVPN”.
- The OpenVPN App starts automatically

- Confirm the import of the file with a tap on the green “+”.
- move the slider to the right to start the connection.
- After successful connection establishment, the VPN symbol appears at the top of the screen & and a counter runs within the app.

iOS

- Download the OpenVPN configuration file for this device in the eBlocker Dashboard (Download Button on the eBlocker Mobile Card)
- Confirm “OPEN FILE” at the bottom of the screen.
- The OpenVPN App opens automatically.
- Confirm the import of the file with “Ok”.
- You are now in the app “OpenVPN”. Move the slider to the right to start the connection.
- A green slider indicates successful connection establishment and a small green icon appears at the top of the screen.

WINDOWS

- Download the OpenVPN configuration file for this device in the eBlocker Dashboard (Download Button on the eBlocker Mobile Card)
- Localize the downloaded OpenVPN configuration file in the folder for downloaded files (file name: eBlocker_Mobile_MyEBlockerovpn)
- Copy the OpenVPN file to the configuration files folder. This is usually c:\tbd
- Start the OpenVPN App. Often it has already started.
- Select the OpenVPN icon in the task bar and there the eBlocker configuration
- your device connects to your eBlocker.

macOS

- Download the OpenVPN configuration file for this device in the eBlocker Dashboard (Download Button on the eBlocker Mobile Card)
- Localize the downloaded OpenVPN configuration file in the folder for downloaded files (file name: eBlocker_Mobile_MyeBlockerovpn)
- double-click the loaded.ovpn file.
- Confirm the installation dialog
- Click the Tunnelblick icon in the menu bar.
- Choose “Connect eBlocker_Mobile_MyEBlocker”
- Your Mac now connects to your eBlocker.

9 Quick guides

9.1 Delete cookies, cache and browsing history in browser

Depending on the browser you are using, you can delete cookies in many different ways. The deleting process for the most important browsers are explained in the following section. If your browser is not listed here, please follow your browser instruction how to delete cookies, cache and browsing history.

9.1.1 Firefox

Open your browser and click on the menu symbol at the right top of your browser. A new browser window with different options will appear.

Click on settings and go to "data protection".

Click on „recent set chronicle". A new window will open in which you can add relevant subjects that you want to have deleted afterwards. We recommend to add following subjects in order to erase your trace completely.

- Visited websites & download chronicles
- Cookies
- Submitted search terms & form data
- Offline website files

Through the link „Today's chronicle" you have the option to set a period of time. We recommend to choose every subject in order to be fully protected against trackers. Finish deleting your browsing history by clicking "delete now".

9.1.2 Chrome

Open your browser and click on the menu icon at the right top of your browser window. Go to settings and click on "history". Finish deleting your browsing history by clicking "delete browsing data". Please note to state the whole period of time.

9.1.3 Internet Explorer

Click on the setting icon at the right top of your browser window. Go to „Internet Options" and to „General" afterwards. Finish deleting your trace by clicking „delete browsing history".

10 Glossary

- **Content lock**

Providers of (e.g.) journalistic content have a legitimate right – and of course the necessity – to make money with their offers. Many providers offer users to pay for the content directly, individually or per subscription – or just to accept that the called up site contains advertisement.

Some providers reserve the right to lock the cost-free service if the user uses an ad-blocker. This lock is also called “content lock”.

eBlocker’s aim is not to destroy the business plan of Internet providers. However, we do block ads from advertising networks for these kind of sites, because nowadays the ad banners are used for profiling. We do not help to avoid the named content lock. Instead we recommend to honor high-quality content on a fair basis, so independent quality journalism is permanently preserved for all of us.

- **Cookies**

Cookies typically contain data about visited websites, that the web browser of this websites saves on your computer and uses the next time you visit the same website again. Cookies however are not fundamentally bad. They can increase the user comfort e.g. if you do not have to sign up again after already having visited the website. Cookies can also be used to recognize the same individual on different websites, so personality profiles can be generated comprehensively.

These tracking cookies are blocked from your eBlocker, so that they cannot even get into your computer.

- **DHCP server and DHCP lease**

The Dynamic Host Configuration Protocol (DHCP) enables the automatic integration of network devices into all networks. A central server – in such case the router - assigns the network configuration to all devices. The lifetime of this assignment is called lease time. The administrator can choose the existence of the lifetime at the router settings. The lease time can be indicated in seconds, days or even weeks. If the DHCP server is changed during operation, all computers/devices must be disconnected from the network once, so every device can be notified by the new DHCP server and thus receives a DHCP lease.

- **Digital certificate**

A digital certificate uses cryptographic methods, to verify the details to a communication partner obligatory. For example, if a certain website is actually run by the named company. Digital certificates are usually issued by trustworthy certification authorities that verified the details and take responsibility for the correctness.

- **DNS Server**

The DNS server (Domain Name System) is some sort of telephone book for the Internet. It translates the server names from URLs and from email addresses to numerically IP addresses. The webserver is identified and spoken to through the IP address.

- **LAN cable**

The LAN cable (Local Area Network) or also called Ethernet cable, is a network cable that is required for connecting the computer and other devices to your local net. Ethernet cables are often yellow colored. The supplied Ethernet cable of eBlocker is obviously orange colored!

- **Malicious software**

Malicious software is the generic term for dangerous computer programs like viruses, worms or Trojans. Malicious software can get into your computer by visiting infected websites or by opening infected emails. Even banner ads that appear on websites which appear as trustworthy may contain the so called “malware” in short. Not every malware is immediately noticed (or at all). The best way to protect yourself from malware is to keep your system as up to date as possible; no opening of suspicious emails that are send from dubious sources; using the latest antivirus program and of course, using your eBlocker.

- **Network mask**

With help of the IP address the network mask defines which other IP addresses belong to the local net. That means which addresses can be reached directly. All other IP addresses that do not belong to one network mask, do not belong to the local network and can only be reached through the router.

- **Price discrimination**

Price discrimination describes a price policy on the Internet, where you get different prices for the same product depending on from which device you want to buy the product. The price is set dynamically according to the known data of the user with the aim to maximize their revenue.

- **Referrer**

If you open a website, your browser sends you an according request for the website you want to visit. This request not only contains the URL, but also many other meta-files for requests. Amongst other things the browser transmits from which website the new request was send from. This indication is called „HTTP-referrer“ or in short „referrer“.

It has the legitimate right, to see insights which sites have been visited by the user and thus can optimize their offers accordingly. The referrer can also be used in a comprehensive way, so personality profiles can be created and connected.

- **SSL Encryption**

SSL (Secure Sockets Layer) encryption is a method of data encryption. In connection with the certificates, it ensures, that no changes can be made to the data on the way from the server to a browser and the data exchange can not be read by unauthorized persons.

If an Internet user logs into a forum or an online shop, his registration data and texts can easily be viewed and later misused when sent without SSL encryption. If the connection is protected by SSL, it would take a relatively high effort to decrypt this encryption.

- **Tor Network**

The Tor network is used to disguise your original IP address and to provide anonymous Internet surfing. Suppose you have a certain page you want to visit and therefore you enter the URL into the web browser. Your IP address is sent directly to the page you want to visit. However, if you use Tor, you will be directed into the Tor network, which is made out of many other IP addresses from different computers. The Tor network will send an IP address to the page that it chooses randomly out of all the other IP addresses floating around the Tor network. This is how your real IP address is disguised.

- **Tracker – Data collector**

Most of the time trackers are service providers for advertising industries. Every time a user opens a site that is being tracked, the tracker gets a notification that a user has been tracked successfully.

Through according cookies or other techniques, the tracker can recognize the user even through many different websites again and again and thus generate a detailed protocol of the Internet behavior. All trackers make their money by providing these personality profiles to advertising industries. The advertising industries can now generate target oriented advertisement and place them on sites that are visited frequently by the user.

- **openPVN**

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure connection.

- **VPN**

A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across the public network as if their computing devices were directly connected to the private network.

Appendix A Technical specifications (not valid for software licenses)

- 1 x 10/100/1000 LAN RJ45
- 1 x Power supply 5V (≥ 2A)
- 1 x Wi-Fi 802.11 b/g/n
- 2 x USB 2.0 (for extensions)
- 1 x HDMI (not in use)
- Power consumption: <10W
- Dimensions: 9x9x9cm
- Weight: ca. 153g

Appendix B Safety notes

Please mind the following safety notes before using your eBlocker.

- Your eBlocker does not have a power switch. A disconnection from the power supply should be possible at any time.
- In case of wall mounting your eBlocker, please ensure that no wires or piping can be damaged behind the mounting surface.
- Please protect your eBlocker from moisture, dust, liquids and vapors.
- Please do not block the air vents of your eBlocker.
- Never disconnect the power supply or network connection during an update. This can damage the eBlocker irreparably.

Appendix C Manufacturer & copyright

eBlocker GmbH
Kaiser-Wilhelm-Str. 47
20355 Hamburg
Germany
www.eBlocker.com

Appendix D Technical support

Web: http://forum.eBlocker.com
Email: support@eBlocker.com

Unfortunately we do not offer any telephone support at the moment.

eBlocker®
Switch on Privacy.

Firmware-Version
eBlocker Base/Pro/Family 2.0_20180830-v36

eBlocker GmbH
All rights reserved. Errors and omissions reserved
eBlocker GmbH | Kaiser-Wilhelm-Str. 47 | 20355 Hamburg | Germany