eBlocker®

Switch on Privacy.

Handbuch

Achtung: Dieses Handbuch ist veraltet. Bitte nur als Referenz verwenden.
Die online Version ist stets aktuell: https://eBlocker.org/docs

eBlocker GmbH

eBlocker GmbH | Kaiser-Wilhelm-Str. 47 | 20355 Hamburg | Deutschland

Inhalt

1 Einführung

Wir freuen uns sehr, dass Sie unseren eBlocker gekauft haben. Seit mehr als drei Jahren wird im Team von erfahrenen Privatsphäre- und IT-Spezialisten daran entwickelt. Wir haben noch sehr viele Ideen und entwickeln derzeit viele weitere Funktionen für Sie, die wir monatlich per Update zur Verfügung stellen. Mit Ihrem Kauf unterstützen Sie unsere Idee von einem freien und privaten Internet. Vielen Dank dafür!

Dieses Handbuch erläutert alle Funktionen des eBlockers und unterstützt Sie bei der Inbetriebnahme. Sollten doch noch Fragen auftauchen, finden Sie unter http://forum.eblocker.com viele Antworten und persönliche Hilfe.

1.1 Die eBlocker Produkte

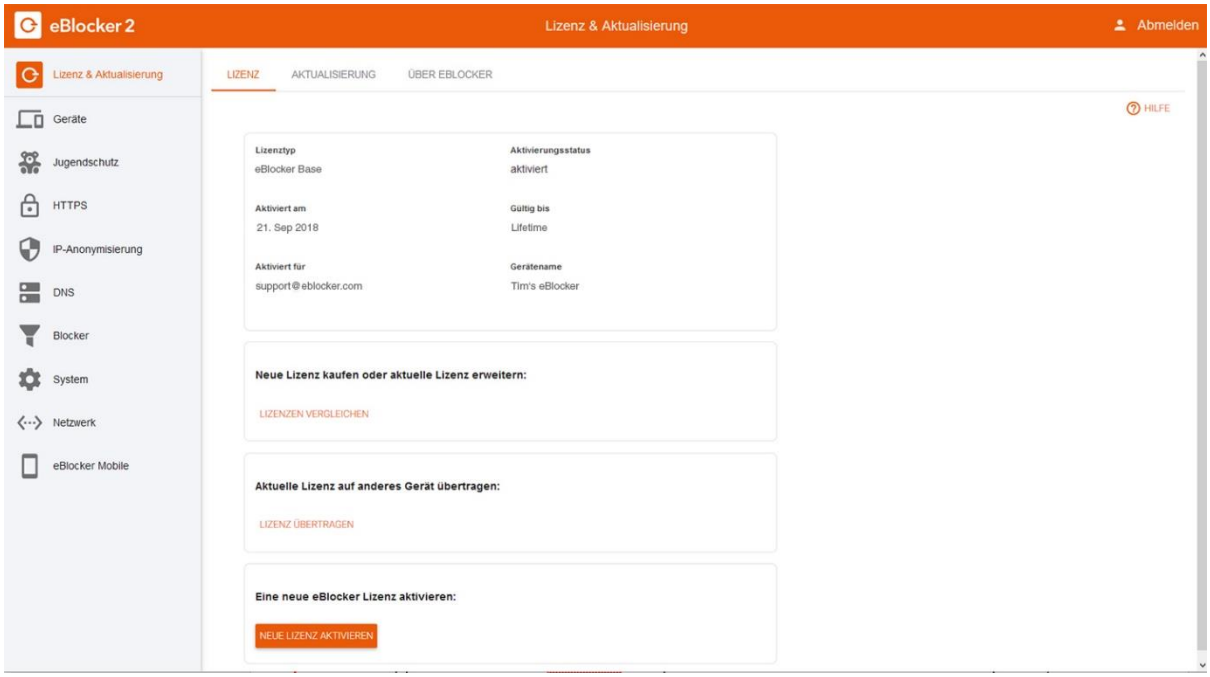
Der eBlocker ist in drei Varianten erhältlich: **eBlocker Base**, **eBlocker Pro** und **eBlocker Family**. Alle Varianten basieren auf derselben technischen Architektur und unterscheiden sich nicht in der Hardware. Die Unterscheidung der Produkte wird softwareseitig bei der Aktivierung der Lizenz festgelegt.

Egal ob **eBlocker Base**, **eBlocker Pro** oder **eBlocker Family**: Ihre Privatsphäre gehört jetzt wieder Ihnen – und nicht den Internet-Konzernen.

1.2 Die eBlocker Varianten

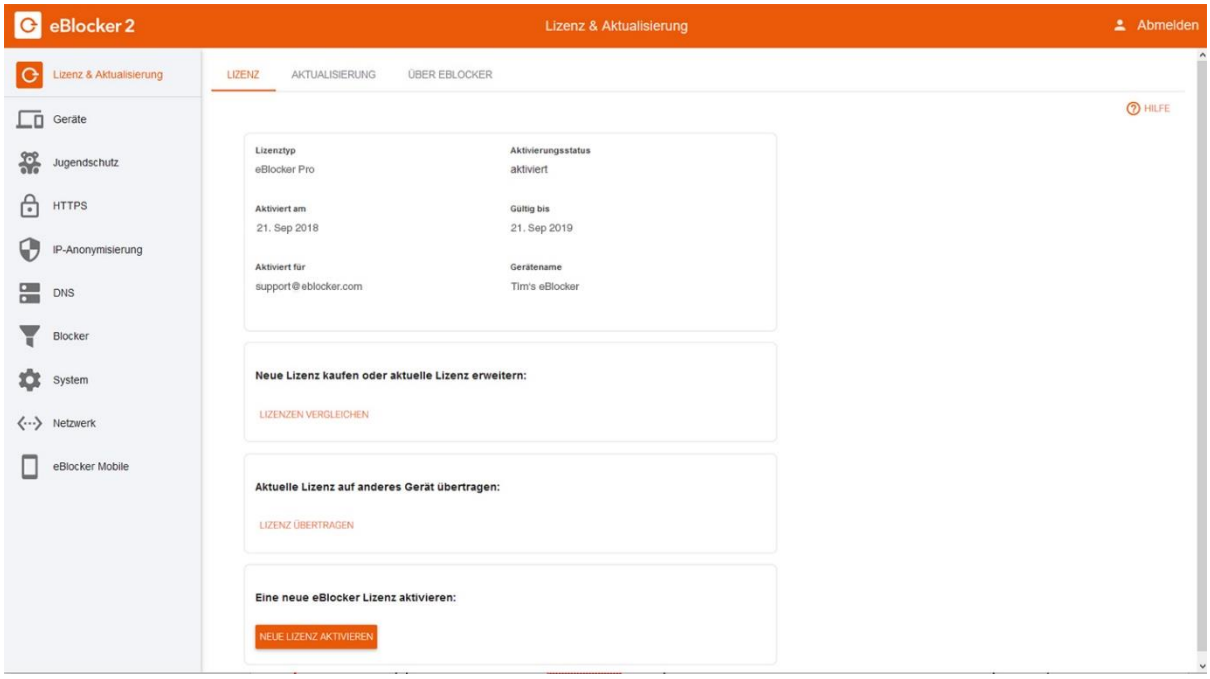
1.2.1 eBlocker Base

Der e**Blocker Base** ist die unkomplizierte Plug & Play-Lösung zum Schutz Ihrer Privatsphäre beim Surfen, bei der Ihre IP-Adresse wirkungsvoll anonymisiert wird. Er kann jederzeit zum **eBlocker Pro** oder **eBlocker Family** erweitert werden.



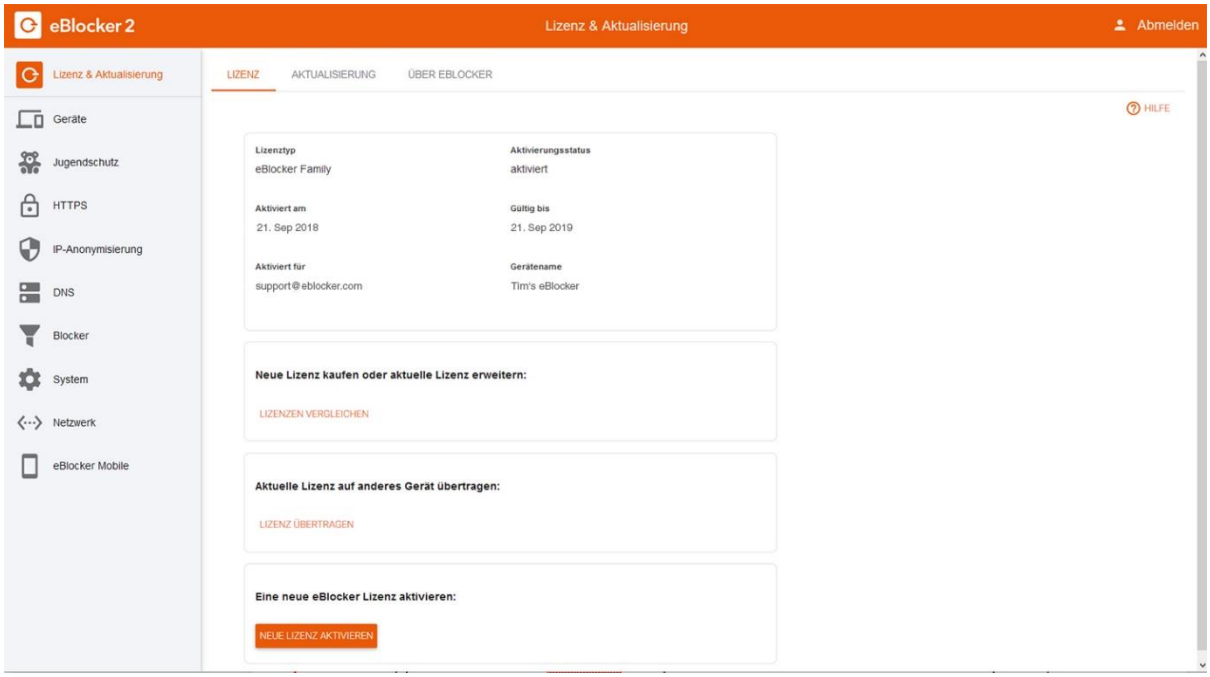
1.2.2 eBlocker Pro

Der **eBlocker Pro** beinhaltet die Funktionen des **eBlocker Base** und filtert Datensammler und datensammelnde Werbung auf allen Geräten und Browsern – sogar wenn Sie unterwegs sind. Der **eBlocker Pro** kann jederzeit zum **eBlocker Family** erweitert werden.



1.2.3 eBlocker Family

Der e**Blocker Family** erweitert die Funktionen des **eBlocker Pro** um individuelle Multi-User Unterstützung und Jugendschutzfunktionen. So schützen Sie jedes Familienmitglied ganz individuell und Ihre Jüngsten vor jugendgefährdenden Inhalten.



Die drei eBlocker Varianten unterscheiden sich nicht von der Hardware und basieren auf der gleichen Software.

Je nach der eBlocker Variante werden in den Einstellungen für Sie Funktionen verfügbar sein oder Sie werden darauf hinweisen, dass diese Funktion zu einer der anderen eBlocker Variante gehört.

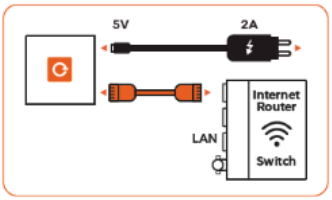
2 Inbetriebnahme

Mithilfe dieses Handbuchs richten Sie Ihren eBlocker im Handumdrehen ein. Folgen Sie den einzelnen Schritten und nehmen Sie das Gerät in angegebener Reihenfolge in Betrieb.

In nur drei Schritten ist Ihr eBlocker einsatzbereit:

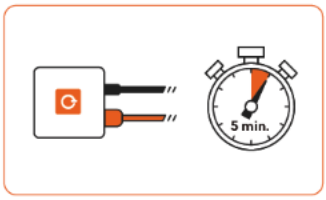
1. Anschluss

Schließen Sie **zuerst** Ihren eBlocker mit dem **orangen LAN-Kabel** an Ihren Router oder Switch an. **Anschließend** verbinden Sie den **eBlocker mit dem Netzteil** und der Stromversorgung.



2. Automatische Konfiguration

Warten Sie **5 Minuten** bis sich der eBlocker automatisch konfiguriert hat. Starten Sie einen Internet-Browser und gehen Sie auf: http://setup.eblocker.com



3. Start

Das eBlocker Icon erscheint oben rechts im Browserfenster. Über die sogenannte „Controlbar“, die Sie durch einen Klick auf das Icon öffnen, können Sie jederzeit die wichtigsten Informationen zur aktuell aufgerufenen Seite einsehen und Einstellungen anpassen. Der Link *Aktivieren* führt Sie zum Aktivierungsassistenten. Falls das Icon nicht erscheint, kann Ihnen im Kapitel 5.4 geholfen werden.

3 Aktivierung

Zur Aktivierung halten Sie bitte die **Seriennummer** Ihres eBlockers und den Lizenzschlüssel sowie Ihre **E-Mail-Adresse** bereit.

Die Seriennummer finden Sie auf dem Typenschild auf dem Karton sowie am Boden des eBlockers. Sie hat das Format „SNXXXXXXXX“. Der Lizenzschlüssel befindet sich auf der **Lizenzkarte**, die dem Gerät beiliegt.

Bitte verwenden Sie eine gültige E-Mail-Adresse bei der Aktivierung. Diese E-Mail-Adresse wird auch benötigt, wenn Sie Ihre eBlocker Lizenz einmal auf ein anderes Gerät übertragen möchten.

Hinweis: Die Zahl „0“ ist nicht im Lizenzschlüssel enthalten. Sollten Sie dieses Zeichen in Ihrem Lizenzschlüssel auffinden, handelt es sich lediglich um den Buchstaben „O“.

4 eBlocker optimal nutzen

4.1 Update

Wir empfehlen den eBlocker vor der Verwendung manuell zu aktualisieren. Um das neueste eBlockerOS-Update manuell zu installieren, klicken Sie auf das eBlocker-Symbol und gehen Sie zu "Einstellungen". Klicken Sie auf "Allgemein". Wählen Sie die Registerkarte "Updates" und klicken Sie auf die Schaltfläche "Jetzt aktualisieren".

4.2 Überblick

Außerdem empfehlen wir folgende Schritte nach der Aktivierung durchzuführen:

- Löschen Sie die Cookies, Cache und Browser Historie in allen verwendeten Browsern.
- Aktivieren Sie SSL (HTTPS-Unterstützung) auf dem eBlocker.
- Nehmen Sie das Zertifikat des eBlocker in Ihrem Betriebssystem und dann ggf. in den Browsern mit einem eigenen Zertifikatsspeicher wie im Abschnitt 6.2 beschrieben auf.
- Aktivieren Sie eventuell Ausnahmelisten für spezielle Apps, die vom Schutz durch den eBlocker ausgenommen werden sollen.
- Definieren Sie eventuell zusätzliche Ausnahmen für verschlüsselte Verbindungen (SSL) – z.B. für Online-Banking –, bei denen der eBlocker nicht aktiv werden soll.

Nachfolgend werden alle Schritte im Detail erklärt.

4.3 Cookies, Cache und Browser Historie löschen

eBlocker verhindert automatisch, dass Daten sammelnde Cookies oder andere Elemente, durch die Sie identifizierbar sind, auf Ihren Browser gelangen. Ohne eBlocker hat Ihr Browser jedoch wahrscheinlich bereits zahlreiche Tracking-Cookies der unterschiedlichsten Anbieter gesammelt. Wir empfehlen daher, zuerst **alle Cookies zu löschen**, damit diese Tracker „Ihre Spur verlieren“.

Wie Sie Cookies in Ihrem jeweiligen Browser löschen beschreiben wir im Abschnitt 9.1.

4.4 Unterstützung für HTTPS/SSL-Verbindungen aktivieren

Wie Sie die Unterstützung für HTTPS/SSL-Verbindungen aktiveren, beschreiben wir in Abschnitt 8.4.1

4.5 Ausnahmen für Apps aktivieren

Die Beschreibung wie Sie Ausnahmen für Apps aktivieren, finden Sie in Abschnitt 8.4.3

4.6 Abschließende Empfehlung

Wir haben den eBlocker sehr sorgfältig entwickelt und verbessern ihn permanent. Trotzdem ist der eBlocker keine „Magic Pill“ für die Privatsphäre, die unter allen Umständen funktioniert. Insbesondere

Apps, die nativ auf Ihrem Endgerät/Betriebssystem laufen, stellen ein erhöhtes Risiko für Ihre Privatspähe dar. Wir empfehlen daher möglichst **keine Apps zu verwenden.**

Apps sind heute sehr verbreitet, um auf Internet-Dienste zuzugreifen. Jedoch bergen sie ein größeres Risiko für Ihre Privatsphäre, als wenn Sie den gleichen Dienst über einen Browser verwenden. Warum Sie zum Schutz Ihrer Privatsphäre auf Apps verzichten sollten, erläutern wir im Folgenden:

Eingriff in Ihre Privatsphäre

Apps wie z.B. Facebook, WhatsApp oder Twitter können direkt auf Daten Ihres Endgerätes zurückgreifen und eigene Kommunikationsprotokolle benutzen, die durch den eBlocker nicht geschützt werden können.

Übertragung von Schadsoftware

Auch die Übertragung von Schadsoftware stellt eine große Gefahr dar. Über die App-Stores werden nicht nur sichere Programme bereitgestellt, sondern immer wieder auch Apps, die mit Schadsoftware infiziert sind. Diese verseuchten Programme können Handy-Daten (z.B. Kontaktdaten) unbemerkt und unbefugt übermitteln oder kostenpflichtige SMS an Servicenummern versenden.

Ausnahmen nur sparsam nutzen

Einige Apps sind nur dann mit dem eBlocker kompatibel, wenn deren Kommunikation nicht durch den eBlocker überwacht wird. Entsprechende Ausnahmelisten für diese Apps können in den Einstellungen unter „Apps“ aktiviert werden, und sie werden dann von der Analyse durch den eBlocker ausgenommen. Mit jeder Ausnahme, die Sie hinzufügen, bekommt der Privatsphäreschutz „Löcher“ und Daten können wieder unbemerkt über Sie erhoben werden.

5 Wenn einmal etwas nicht funktioniert

Trotz der einfachen Plug & Play Lösung des eBlockers können vereinzelt Inkompatibilitäten auftauchen, die unterschiedliche Ursachen haben können. Nachstehend haben wir einige Punkte zusammengefasst, die Ihnen weiterhelfen, wenn einmal etwas nicht funktioniert.

5.1 Verbindungs- und Netzwerkprobleme

- **Netzwerk individuell einstellen**

Bei Erstanschluss befindet sich Ihr eBlocker standardmäßig im automatischen Netzwerkmodus. Dieser Modus ist mit den meisten Netzwerkgeräten kompatibel. Sollten dennoch Verbindungsfehler auftreten oder sich die Geschwindigkeit im Netzwerk reduzieren, können Sie den eBlocker für Ihr Netzwerk mit wenigen Klicks individuell eingestellen. Damit werden in der Regel alle Netzwerkprobleme sofort behoben. Wie Sie Ihr Netzwerk im eBlocker individuell einstellen ist im Kapitel 8.9 beschrieben.

5.2 Eine Webseite wird nicht angezeigt

Wenn der eBlocker grundsätzlich funktioniert, jedoch Störungen auf bestimmten Webseiten auftreten, haben wir hier einige Tipps für Sie zusammengefasst:

- **eBlocker pausieren**

Klicken Sie hierfür auf das eBlocker Icon oben rechts in Ihrem Browserfenster. Mit der Funktion „Pause“, können Sie den eBlocker für das Gerät, das Sie gerade nutzen, für einige Minuten pausieren. Versuchen Sie die gewünschte Webseite anschließend noch einmal neu zu laden. Wenn die Pausefunktion Abhilfe geschafft hat und Sie die Webseite häufig besuchen, empfehlen wir eine Ausnahme für diese Website hinzuzufügen.

- **Ausnahmen hinzufügen (Whitelisting)**

Gültig für **eBlocker Pro** und **eBlocker Family**

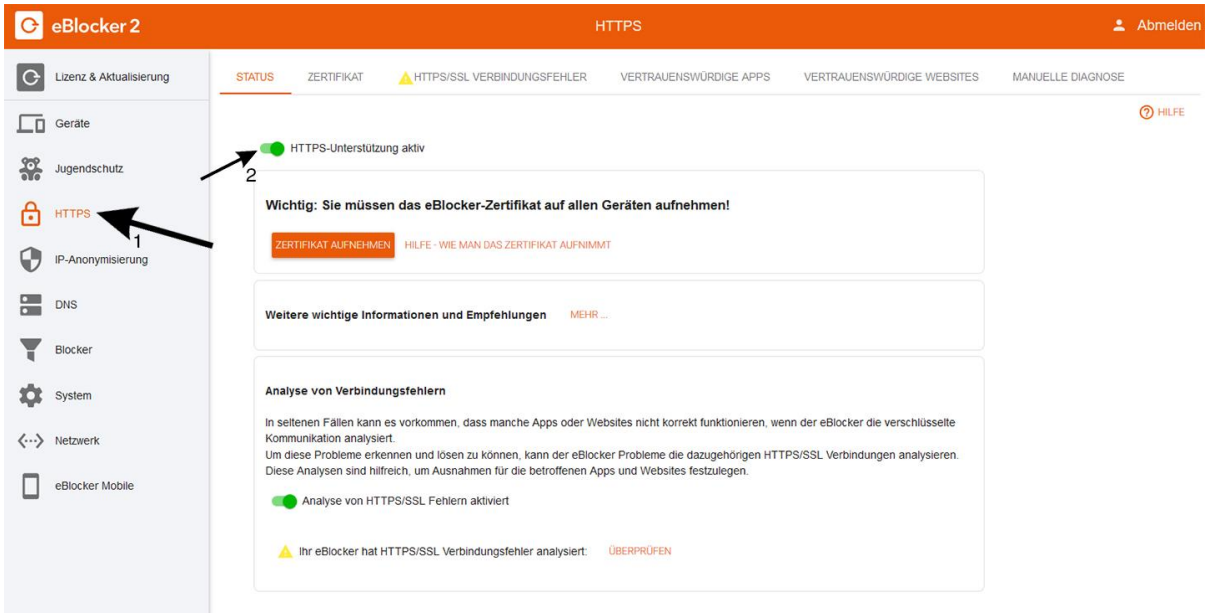
Falls Sie eine Webseite nicht sehen können oder von der Ansicht der Webseite ausgesperrt werden, können Sie für diese Webseite Ausnahmen hinzufügen. Wie Sie diese Ausnahmen hinzufügen, haben wir im Kapitel 8.4.1 beschrieben.

- **HTTPS komplett oder für einzelne Geräte deaktivieren**

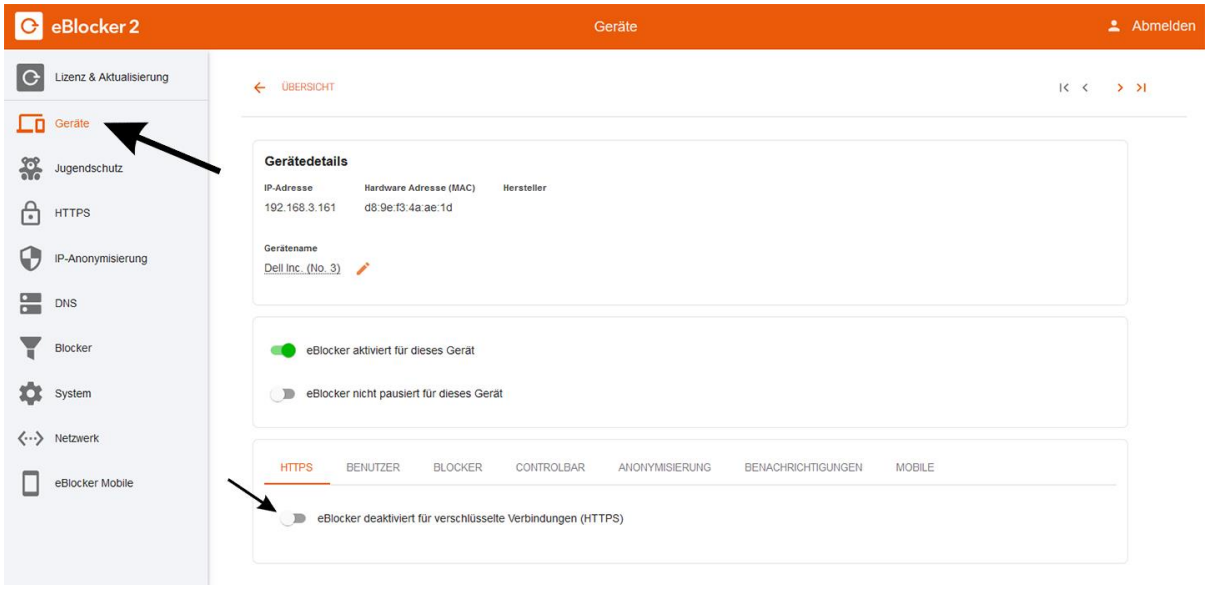
Gültig für **eBlocker Pro** und **eBlocker Family**

In seltenen Fällen kann es vorkommen, dass einzelne mit HTTPS geladene Webseiten oder Apps nicht mit dem eBlocker kompatibel sind. Sie können das leicht überprüfen, indem Sie die HTTPS Funktion auf dem gesamten eBlocker oder nur für das aktuelle Gerät deaktivieren.

Um die HTTPS Funktion komplett zu deaktivieren, öffnen Sie die eBlocker Controlbar. Gehen Sie auf die Einstellungen und klicken Sie anschließend auf „HTTPS“. Deaktivieren Sie die SSL-Funktion mit einem Klick auf den orangen Schiebeschalter, neben dem Schriftzug „HTTPS Unterstützung“.



Um die HTTPS Funktion nur auf einem bestimmten Gerät zu deaktivieren, gehen Sie bitte wie folgt vor. Klicken Sie in den Einstellungen auf Geräte. Suchen Sie das Gerät auf dem die HTTPS Funktion deaktiviert werden soll. Ihr aktuelles Gerät wird immer als erstes in der Liste angezeigt.



Öffnen Sie die Einstellungen für das gewünschte Gerät mit einem Klick auf die entsprechende Zeile und deaktivieren Sie HTTPS für das Gerät mit dem gezeigten Schiebeschalter.

■ HTTPS für einzelne Webseiten oder Apps deaktivieren

Falls das Problem durch das Abschalten von der HTTPS Funktion auf dem eBlocker behoben wurde, kann die entsprechende Webseite permanent in eine Ausnahmeliste aufgenommen werden.

Prüfen Sie zunächst in dem Menü „HTTPS“ > Reiter „Vertrauenswürdige Apps“, ob es bereits eine vordefinierte Liste von Ausnahmen für die fragliche App gibt und ob die entsprechende Website in dieser Ausnahmeliste auftaucht. Falls ja, aktivieren Sie die Ausnahmeliste mit ihrem Schalter.

Alternativ können Sie die Website auch einzeln als Ausnahme festlegen. Weitere Informationen, wie Sie Ausnahmen für einzelne Websites festlegen oder wie Sie Ausnahmelisten verwalten, finden Sie in Abschnitt 8.4.1.

5.3 Das eBlocker Icon erscheint nicht auf allen Geräten

Falls der eBlocker grundsätzlich korrekt arbeitet, jedoch das eBlocker Icon nicht auf allen Geräten angezeigt wird, haben wir hier einige Punkte zusammengefasst, die weiterhelfen können.

- **Gerät aktivieren**

Öffnen Sie Ihr Browserfenster und klicken Sie auf das eBlocker Icon. Gehen Sie auf „Einstellungen“ und anschließend auf „Geräte“. Auf der rechten Seite sehen Sie die Liste aller Geräte, die mit dem eBlocker in Ihrem Heimnetzwerk verbunden sind. Sehen Sie nach, ob Ihr Gerät bzw. der Gerätehersteller oder IP-Adresse angezeigt wird. Wie Sie Ihr Gerät aktivieren, lesen Sie im Abschnitt 8.3.3.

- **Das eBlocker Icon anzeigen lassen**

Öffnen Sie Ihr Browserfenster und klicken Sie auf das eBlocker Icon. Gehen Sie auf „Einstellungen“ und anschließend auf „Geräte“. Auf der rechten Seite sehen Sie die Liste aller Geräte, die mit dem eBlocker in Ihrem Heimnetzwerk verbunden sind. Klicken Sie auf die IP-Adresse bzw. dessen Hersteller und sehen Sie nach, ob für Ihr Gerät das eBlocker Icon angezeigt wird. Wie Sie das eBlocker Icon für ein Gerät aktivieren oder deaktivieren, können Sie im Kapitel 8.3.8 nachlesen.

5.4 Das eBlocker Icon erscheint auf keinem Gerät

- **eBlocker neu starten**

Wenn Sie den eBlocker zum allerersten Mal anschließen und nach 5 Minuten Wartezeit auf http://setup.eblocker.com kein Icon erscheint, starten Sie bitte den eBlocker neu. Dazu trennen Sie das Gerät von der Stromversorgung, warten 30 Sekunden und verbinden es anschließend wieder mit dem Netzteil.

- **Cookies und Cache löschen und Seite neu laden**

Löschen Sie die Cookies und den Cache Ihres Browsers oder halten Sie die Shift-/Umschalt-Taste gedrückt, während Sie auf das Browsersymbol für „Seite neu laden“ klicken. Wie Sie die Cookies in Ihrem Browsers löschen ist in Abschnitt 9.1 beschrieben.

Bitte beachten Sie, dass der eBlocker beim erstmaligen Aktivieren 5 Minuten benötigt, um sich automatisch zu konfigurieren.

- **Gerät aktivieren**

Stellen Sie sicher, dass Ihr Endgerät unter „Einstellungen/Geräte“ angezeigt wird und aktiviert ist. Wie Sie Geräte aktivieren, ist im Kapitel 8.3.3 beschrieben. Ist das Endgerät aktiviert, aber das Icon wird nicht angezeigt, folgen Sie bitte Abschnitt 5.3.

5.5 Allgemeine Probleme beseitigen

- **Kabel korrekt einstecken**

Bitte vergleichen Sie Ihren Lieferumfang mit Ihrer Lieferung. Vergewissern Sie sich, dass Ihr Lieferumfang vollständig ist und prüfen Sie, dass Sie nur die beiliegenden Kabel und das Netzteil verwenden und alle Kabel *richtig und fest* eingesteckt sind.

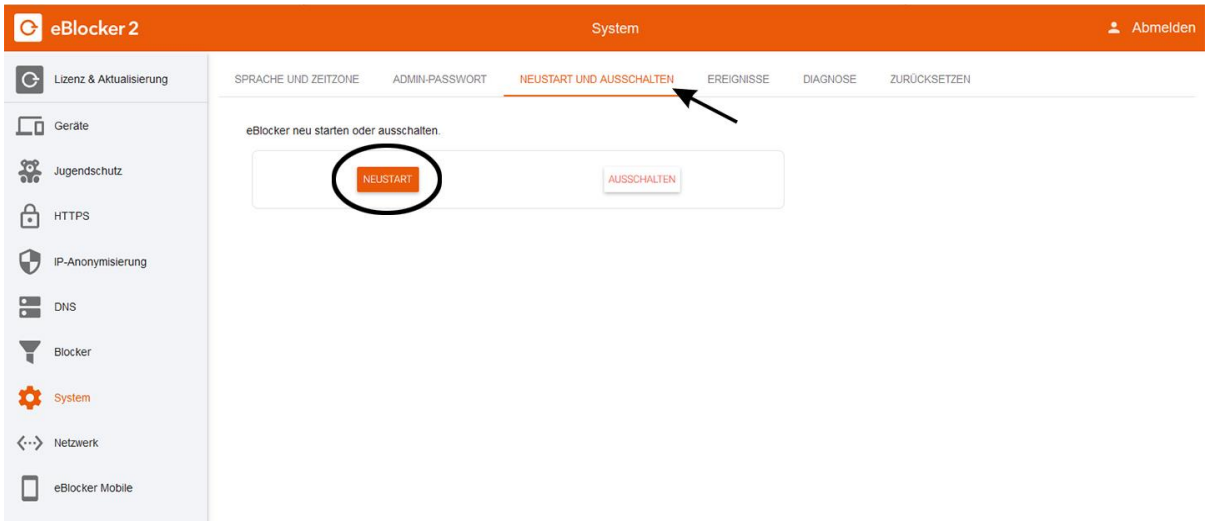
- **Kabel in richtige Anschlüsse stecken**

Bitte stellen Sie sicher, dass das LAN-Kabel tatsächlich in den „LAN“ Port (Anschluss) des eBlockers eingesteckt ist und das Netzteil in den „Power“-Anschluss. Der „HDMI“ Port sowie die USB-Anschlüsse sind für spätere Erweiterungen und derzeit nicht in Funktion.

Bitte beachten Sie auch, dass einige Router eingeschränkte LAN Ports für Gäste besitzen, die für den eBlocker nicht verwendet werden können. Diese Ports sind häufig LAN1 oder LAN4/LAN5. Bitte verbinden Sie den eBlocker mit einem der anderen Ports Ihres Routers.

- **eBlocker neu starten**

Öffnen Sie Ihren Browser und klicken Sie oben rechts auf das eBlocker Icon. Gehen Sie auf Einstellungen und klicken Sie anschließend auf „System“.



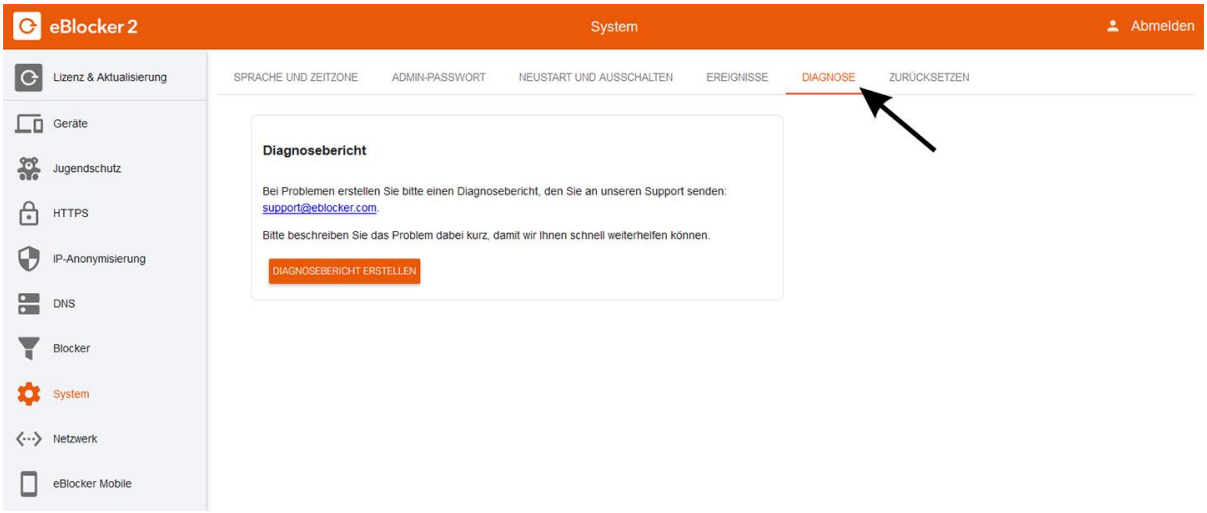
Der Reiter „Neustart und Herunterfahren ist bereits orange unterlegt. Klicken Sie auf den Button „Neustart“. Ihr eBlocker startet selbst neu.

Sollten die eBlocker Einstellungen nicht erreichbar sein, können Sie das Gerät auch durch Unterbrechen der Stromversorgung neu starten. Bitte warten Sie 30 Sekunden, bis Sie das Gerät wieder mit Strom versorgen.

Bitte beachten Sie, dass der eBlocker nach dem Neustart 5 Minuten benötigt, um das Netzwerk zu erkennen und sich selbst zu konfigurieren.

- **Diagnosebericht an Support-Team senden**

Im Fehlerfall oder bei Problemen können Sie einen automatisierten Diagnosebericht erstellen, den Sie an uns senden können (Abschnitt Anhang D). Durch den Diagnosebericht können wir genau erkennen in welchem Zustand sich das Gerät befindet und so eine schnelle Lösung im Fehlerfall finden.



- **Router neu starten**

Fahren Sie Ihren Router herunter und starten Sie ihn erneut. Beachten Sie dabei das Benutzerhandbuch Ihres Routers. Häufig genügt es für einen Neustart, den Router kurz von der Stromversorgung zu trennen und ihn anschließend wieder mit Strom zu versorgen.

5.6 Einige Apps funktionieren nicht

Anders als normale Browser haben Apps mehr Zugriffsmöglichkeiten und „Freiheiten“ auf Ihrem Gerät. Während die meisten Browser und Websites problemlos zusammen mit Ihrem eBlocker funktionieren, können vereinzelt Inkompatibilitäten mit Apps auftreten.

Insbesondere wenn der eBlocker auch für verschlüsselte Verbindungen (HTTPS) aktiviert ist, kann es bei einzelnen Apps zu Problemen kommen. In der Regel lassen sich die Probleme leicht beseitigen, wenn die entsprechenden Websites, mit denen die App per HTTPS (SSL) kommuniziert, von der Analyse durch den eBlocker ausgenommen werden.

Für einige der am weitesten verbreiteten Apps gibt es bereits vorbereitete Ausnahmelisten, die Sie im Menü „HTTPS“ > Reiter „Vertrauenswürdige Apps“ einsehen und aktivieren können.

Sie können aber auch eigene Ausnahmelisten für weitere Apps definieren oder die bestehenden Ausnahmelisten bearbeiten und ergänzen.

Insbesondere bei Apps ist es nicht immer ganz einfach herauszufinden, welche Websites von der App tatsächlich angesprochen werden. Um hier die Analyse zu erleichtern, kann der eBlocker in dem Menü „HTTPS“ > Reiter „HTTPS/SSL Verbindungsfehler“ auch Verbindungsfehler automatisch anzeigen. Der eBlocker stellt zudem ein „Expertentool“ zur Aufzeichnung und Auswertung der Verbindungen zur Verfügung und macht Vorschläge, welche Websites in die Ausnahmeliste aufgenommen werden sollten. Dieses Expertentool, oder auch die Manuelle Diagnose, ist im Abschnitt **Fehler! Verweisquelle onnte nicht gefunden werden.** beschrieben.

Aber keine Sorge: Wenn Sie kein Experte sind, schreiben Sie bitte einen kurzen Beitrag in unser Forum (forum.eblocker.com). Teilen Sie uns einfach mit, welche App bzw. welche Funktion einer App zusammen mit dem eBlocker nicht funktioniert. Vielleicht hat ein anderes Mitglied schon genau dasselbe Problem gelöst und kann Ihnen weiterhelfen.

Bitte beachten Sie, dass der eBlocker Sie bei der Verwendung von Ausnahmelisten für Apps auf den entsprechenden Websites nicht schützen kann. Auch dann nicht, wenn Sie gar nicht mit der App sondern mit einem Webbrowser darauf zugreifen.

Bitte lesen Sie im Zusammenhang mit Apps auch unsere Empfehlungen in Abschnitt 4.6.

5.7 Der eBlocker funktioniert überhaupt nicht mehr

Sehen Sie bitte nach, ob bei Ihrem Router der DHCP Server aktiviert ist. Wenn nicht, dann aktivieren Sie ihn bitte.

Nehmen Sie nun den eBlocker aus Ihrem Netzwerk heraus, trennen den eBlocker vom Netzteil und trennen Sie bei allen Ihren aktiven Geräten (PC, Notebook, Smartphone, etc.) kurz das Netzwerk. Gegebenenfalls können Sie auch bei den meisten Geräten in den Netzwerkeinstellungen den „DHCP Lease“ erneuern lassen (vergleichen Sie dazu Abschnitt 6.1). Ihre Geräte sind nun wieder mit dem Internet verbunden.

Trennen Sie nun das Netzwerkkabel von Ihrem Rechner und deaktivieren Sie ggf. auch das WLAN an Ihrem Rechner. Nun schließen Sie den eBlocker mit dem Netzwerkkabel direkt an Ihren Rechner an, verbinden Sie den eBlocker mit dem Netzteil und warten ca. 5 Minuten. Danach rufen Sie die Notfall-IP-Adresse des eBlockers in Ihrem Browser auf: http://169.254.94.109:3000

Mit der Notfall-IP-Adresse gelangen Sie in die Einstellungen des eBlockers. Stellen Sie in den „eBlocker Einstellungen > Netzwerk“ das Netzwerk auf „Automatisch“ und speichern Sie die Einstellung. Gegebenenfalls wird der eBlocker neu starten. Warten Sie den Neustart ab und fahren Sie dann den eBlocker in den „eBlocker Einstellungen > System“ herunter.

Trennen Sie nun den eBlocker von Ihrem Rechner und vom Strom. Vergessen Sie nicht Ihren Rechner wieder mit dem Netzwerk zu verbinden oder ggf. das WLAN wieder zu aktivieren. Nun können Sie den eBlocker wieder an Ihren Router anschließen und ihn mit dem Netzteil verbinden.

5.8 Weitere Hilfe: Unser Forum und Support

Viele hilfreiche Antworten auf die meisten Fragen finden Sie auch in unserem Forum unter http://forum.eBlocker.com

Gerne unterstützen wir Sie auch per E-Mail (siehe Anhang D).

6 Tipps und Tricks

6.1 Die individuelle Einstellung - Der eBlocker übernimmt den DHCP Server

Gültig für **eBlocker Base**, **eBlocker Pro** und **eBlocker Family**

Sie haben den eBlocker angeschlossen und seitdem gibt es Probleme in Ihrem Netzwerk?

Das kann daran liegen, dass Sie einen Router verwenden, der nicht sofort mit dem Plug & Play des eBlocker kompatibel ist.

Sie müssen dennoch nicht auf den Schutz des eBlockers verzichten und können mit nur vier einfachen Schritten den eBlocker in Betrieb nehmen.

Falls Sie einen Begriff einmal nicht verstehen, finden Sie im Glossar unseres Handbuchs Erläuterungen für alle Fachbegriffe.

- Klicken Sie nun in den „eBlocker Einstellungen > Netzwerk“ auf den Netzwerk Assistenten.
- Lesen Sie sich die Vorbereitung durch und klicken Sie in dem Netzwerk Assistenten auf den Button „Weiter“.
- Lesen Sie sich den Ablauf durch und klicken Sie auf den Button „Weiter“.
- Notieren Sie sich unbedingt die nun angezeigten Einstellungen oder drucken Sie diese bitte aus. Dann klicken Sie auf den Button „Weiter“.

  Bestätigen Sie im letzten Schritt, dass Sie alle angezeigten drei Schritte machen werden und klicken Sie auf „Ausführen und Neustart“.

  Der eBlocker ist nach dem Neustart fertig konfiguriert und nun muss nur noch Ihr Router umgestellt werden.
- Loggen Sie sich auf Ihrem Router als Administrator ein.
- Bei einigen Routern müssen Sie die Ansicht der Einstellungen umstellen (zum Beispiel von Standard auf Erweitert).
- Deaktivieren Sie nun den DHCP Server Ihres Routers und speichern Sie die Einstellungen.

  Zum Abschluss müssen Sie bei allen aktuell in Ihrem Netzwerk befindlichen Endgeräten (Rechner, Notebook, Smartphone, etc.) den sogenannten DHCP Lease erneuern. Das ist wichtig, denn sonst nutzen diese Geräte noch die alte Netzwerkinformation.

  Den neuen DHCP Lease bekommen Sie ganz einfach, indem Sie zum Beispiel einmal kurz die Netzwerkverbindung an den Endgeräten trennen. Einige Geräte bieten auch einen Button „DHCP Lease erneuern“ in den Netzwerkeinstellungen an.

  Wichtig: Wenn Sie diese Einstellungen rückgängig machen wollen, müssen Sie erst an Ihrem Router den DHCP Server wieder aktivieren und anschließend den DHCP Server des eBlockers deaktivieren, bzw. die Netzwerkeinstellung des eBlockers auf „Automatisch“ setzen.

6.2 Die Aufnahme des eBlocker-Zertifikats

Wir empfehlen unseren Kunden das eBlocker-Zertifikat erst im Betriebssystem zu hinterlegen, da die meisten Browser und Programme dort das eBlocker-Zertifikat erwarten. Einzelne Programme haben einen eigenen Zertifikatsspeicher. Auf einige dieser Programme werden wir im Anschluss eingehen.

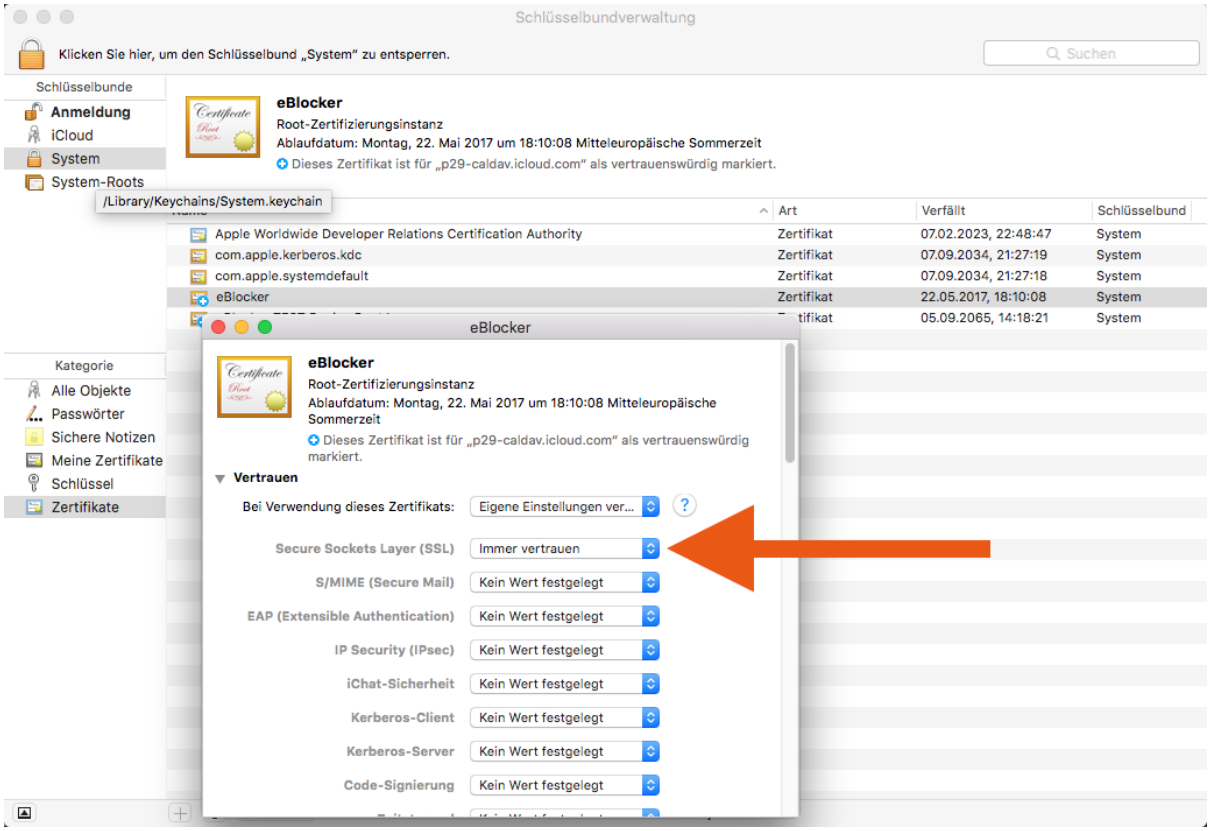
6.2.1 macOS

Mit nur wenigen Schritten haben Sie das Zertifikat hinterlegt. Benutzen Sie dafür bitte den Safari Browser.

Öffnen Sie die eBlocker HTTPS Konfigurationsseite.

Klicken Sie auf den Button *Zertifikat aufnehmen*, um das eBlocker-Zertifikat zu speichern.

- Öffnen Sie die Schlüsselbundverwaltung unter Programme/Dienstprogramme.
- Wählen Sie Schlüsselbund *System* und die Kategorie *Zertifikate* aus.
- Wählen Sie im Menü *Ablage* / *Objekte importieren…* aus.
- Im Datei-Dialog wählen Sie das heruntergeladene eBlocker-Zertifikat aus Ihrem Downloads Ordner und klicken Sie auf *Öffnen*.
- Eventuell werden Sie nach dem Administrator Passwort gefragt.
- Doppel-klicken Sie auf das importierte eBlocker-Zertifikat.
- Wählen Sie *Immer vertrauen* in der Auswahlbox *Secure Sockets Layer (SSL)* aus.
- Schließen Sie das Fenster. Geben Sie bitte das Administrator Passwort ein, nach dem Sie eventuell gefragt werden.



Das eBlocker-Zertifikat ist nun in macOS hinterlegt. Die meisten Browser und Programme können jetzt auf das eBlocker-Zertifikat zugreifen.

Mit den folgenden Browsern können Sie die eBlocker Controlbar nun auf HTTPS Seiten sehen:

- Safari
- Google Chrome
- Opera
- Vivaldi
- Yandex

Für folgende Browser und Programme muss das eBlocker-Zertifikat in dem betreffenden, eigenen Zertifikatsspeicher hinterlegt werden:

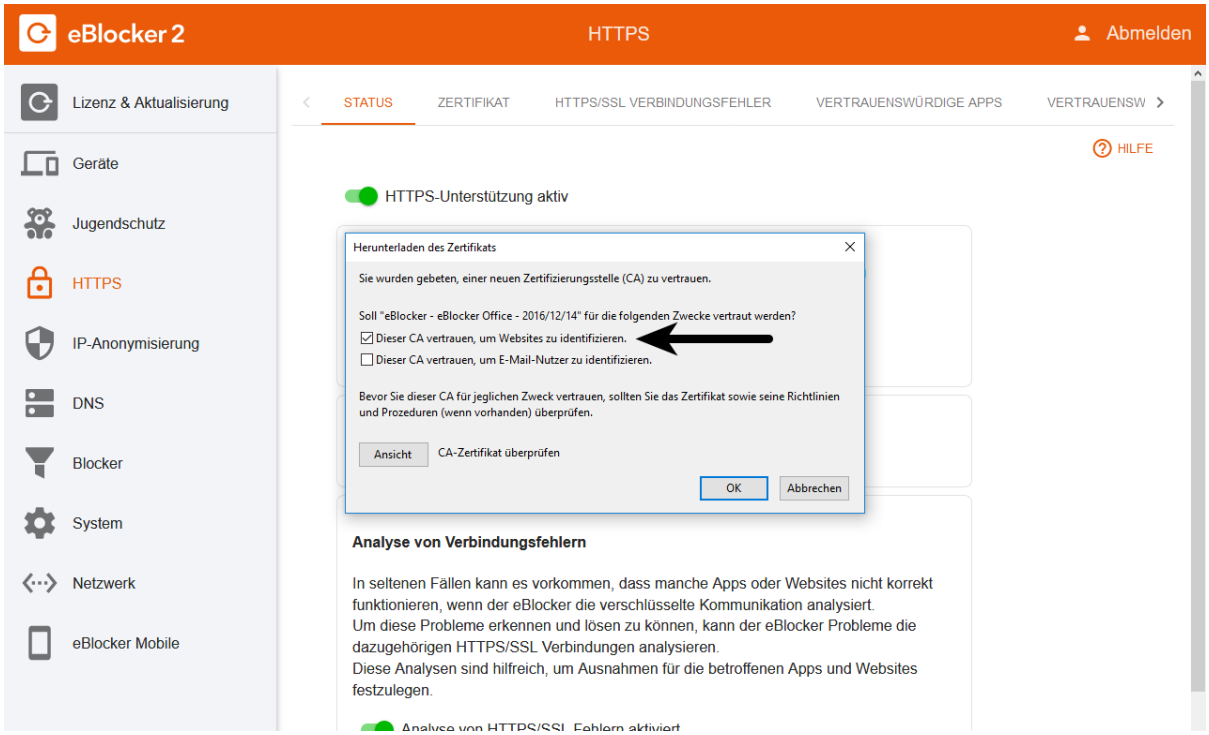
- Firefox
- Cliqz (basiert auf Firefox)
- Seamonkey
- Thunderbird (E-Mail Programm)

Firefox, Cliqz und Seamonkey

Öffnen Sie die eBlocker HTTPS Konfigurationsseite.

Klicken Sie auf den Button *Zertifikat aufnehmen.*

Stellen Sie sicher, dass die erste Checkbox '*Dieser CA vertrauen, um Websites zu identifizieren*' ausgewählt ist (siehe Bilddarstellung).

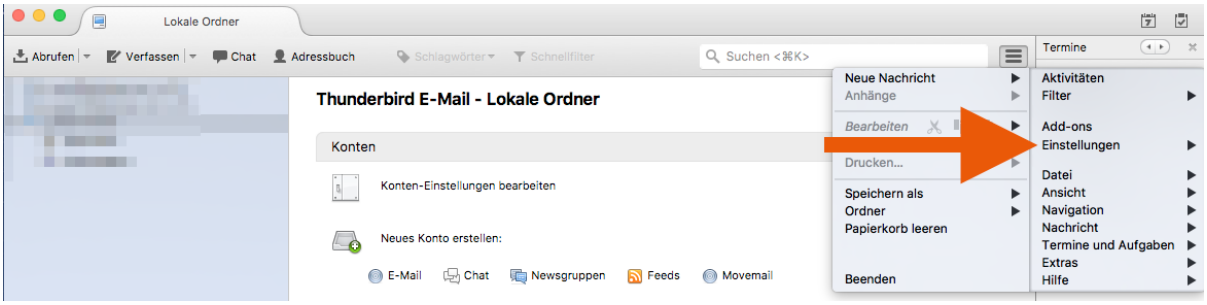


Klicken Sie auf *OK* um das eBlocker-Zertifikat in Firefox aufzunehmen.

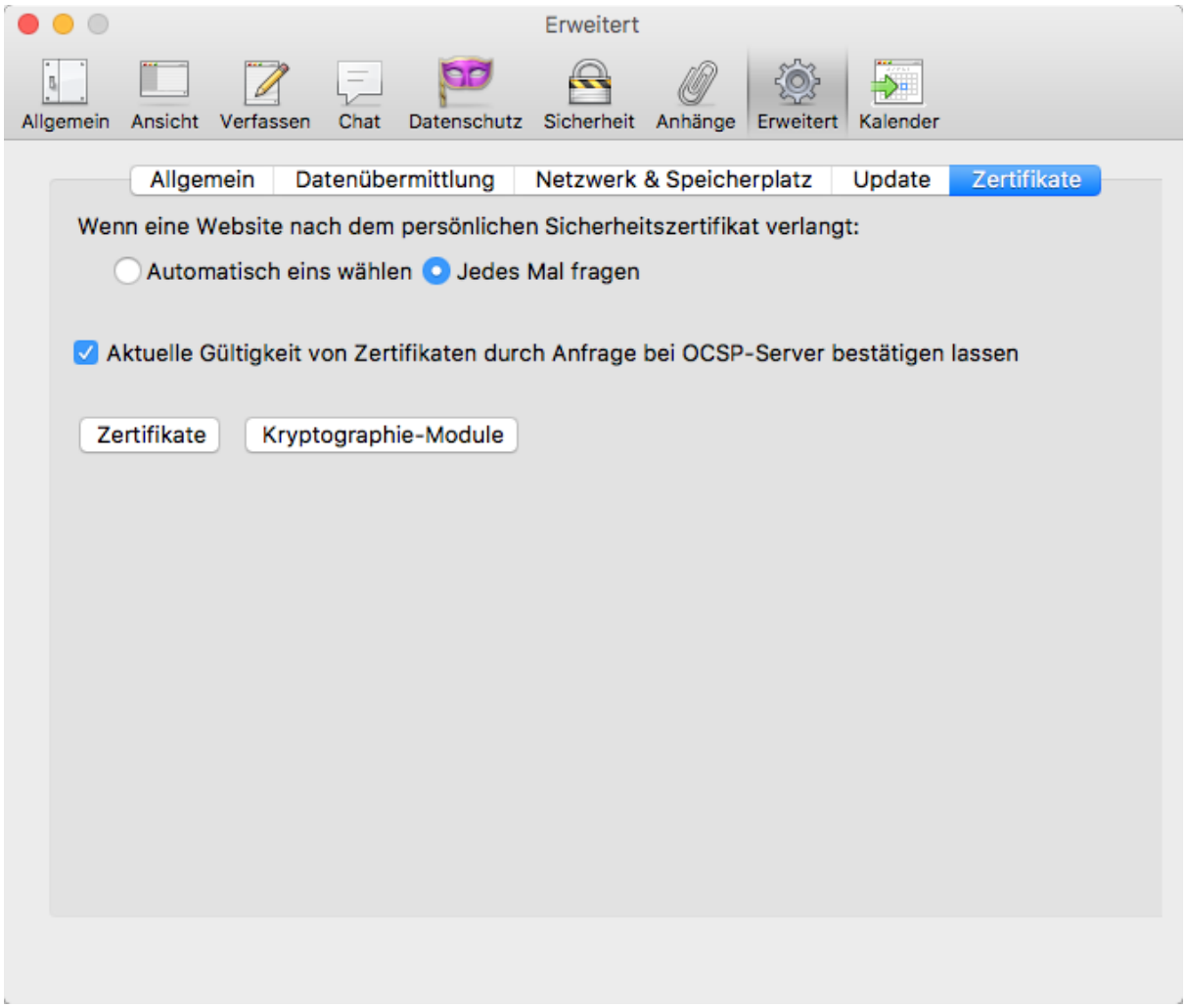
Sie sehen im Firefox, Cliqz oder Seamonkey Browser nun die eBlocker Controlbar auf HTTPS Seiten

Thunderbird (E-Mail Programm)

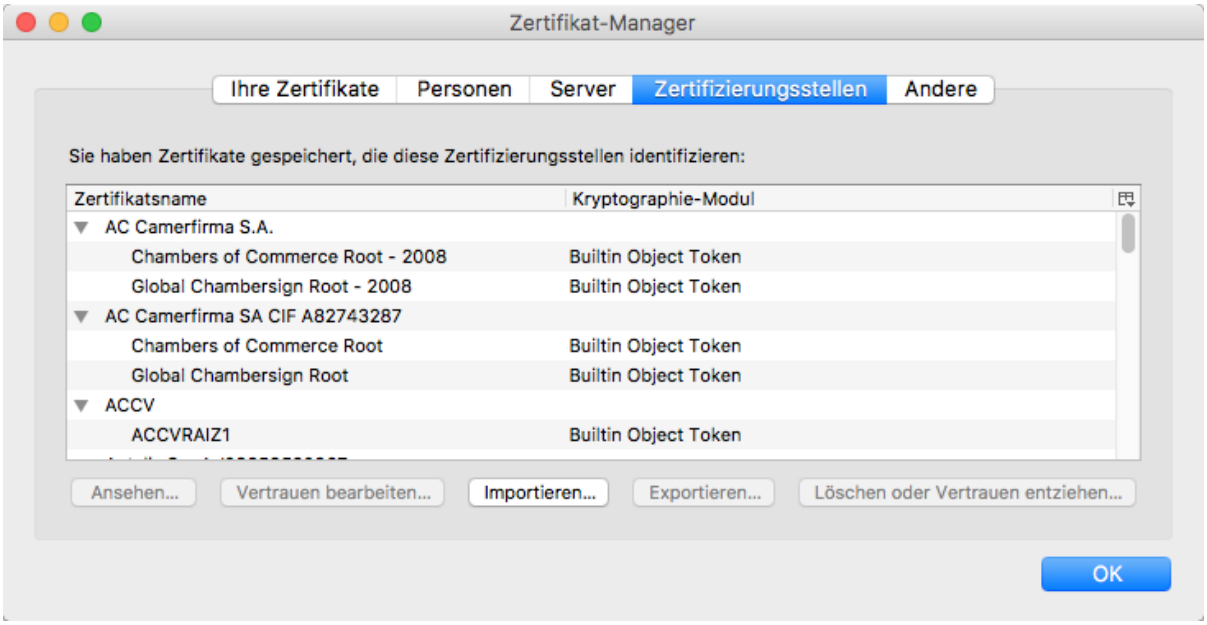
Rufen Sie in Thunderbird das Menü *Einstellungen* auf.



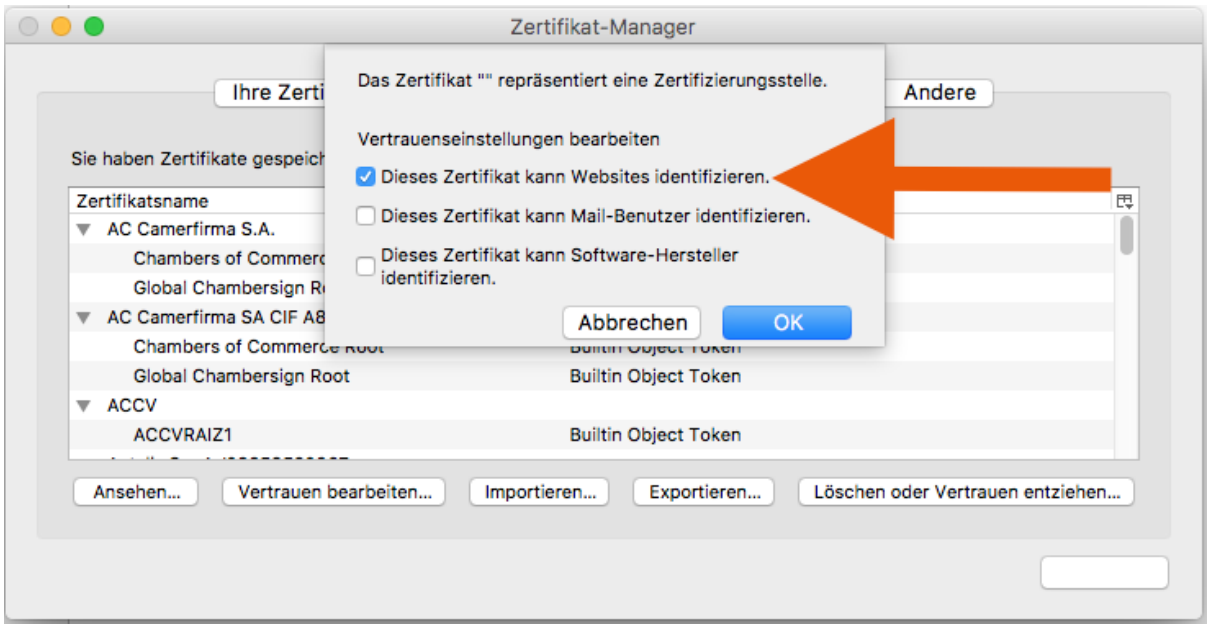
Wählen Sie *Erweitert* aus und klicken Sie auf *Zertifikate*.



Es öffnet sich der Zertifikat-Manager. Dort klicken Sie bitte auf *Importieren* und wählen anschließend das eBlocker Zertifikat aus dem Download Verzeichnis aus.



Laden Sie das eBlocker-Zertifikat mit *Öffnen* und stellen Sie sicher, dass im folgenden Dialog die erste Checkbox '*Dieser CA vertrauen, um Websites zu identifizieren*' ausgewählt ist und bestätigen Sie mit *OK*.



Klicken Sie nun im Zertifikat-Manager auf *OK* und bestätigen Sie die Einstellungen mit *OK*.

Das Zertifikat ist nun im Thunderbird E-Mail-Programm hinterlegt.

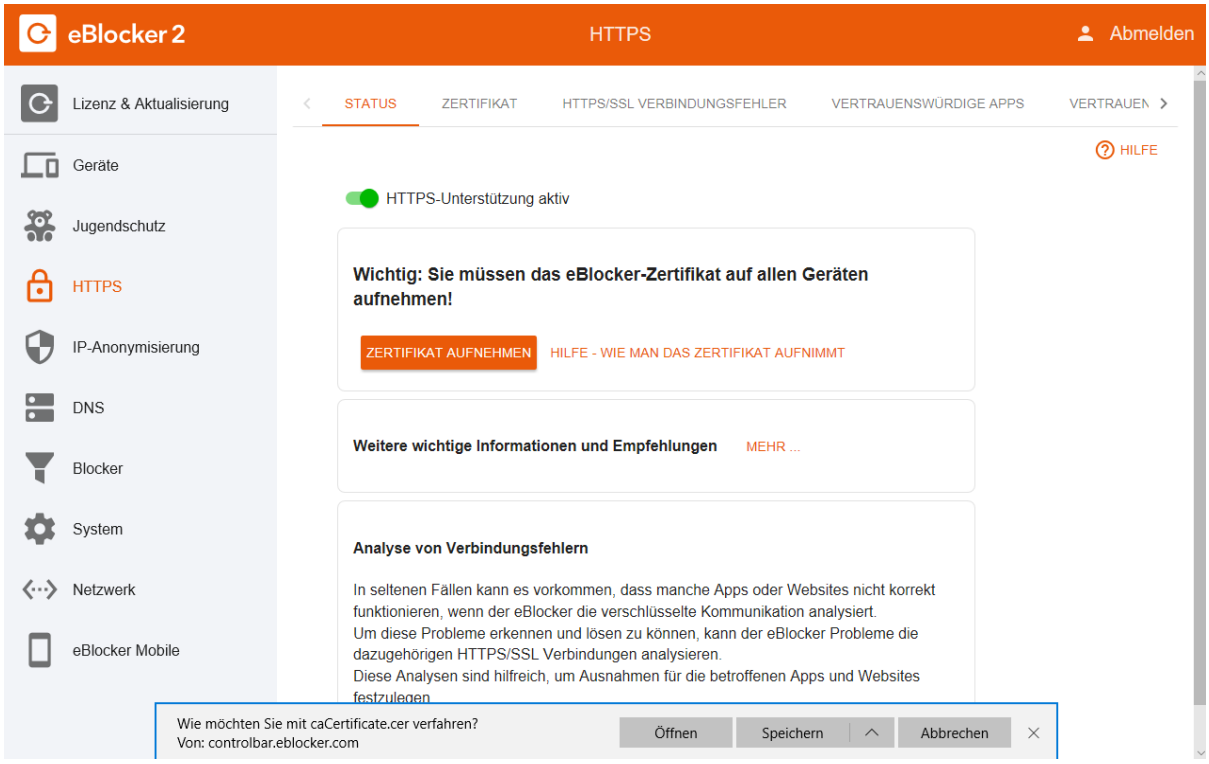
6.2.2 Windows

Mit nur wenigen Schritten haben Sie das Zertifikat hinterlegt. Benutzen Sie bitte den Microsoft Internet Explorer oder den Edge Browser.

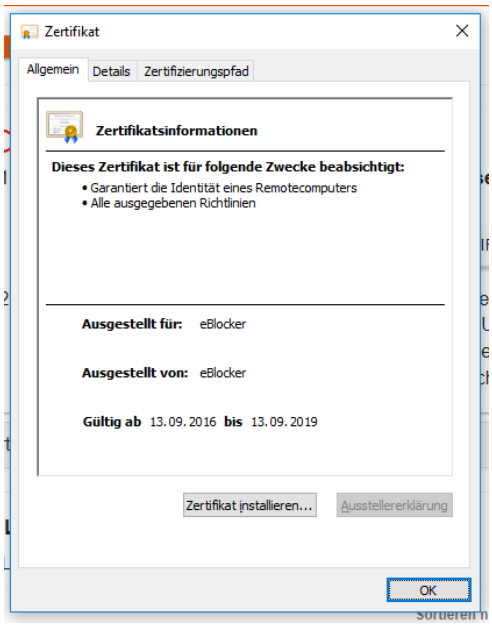
Öffnen Sie die eBlocker HTTPS Konfigurationsseite.

Klicken Sie auf den Button *Zertifikat aufnehmen.*

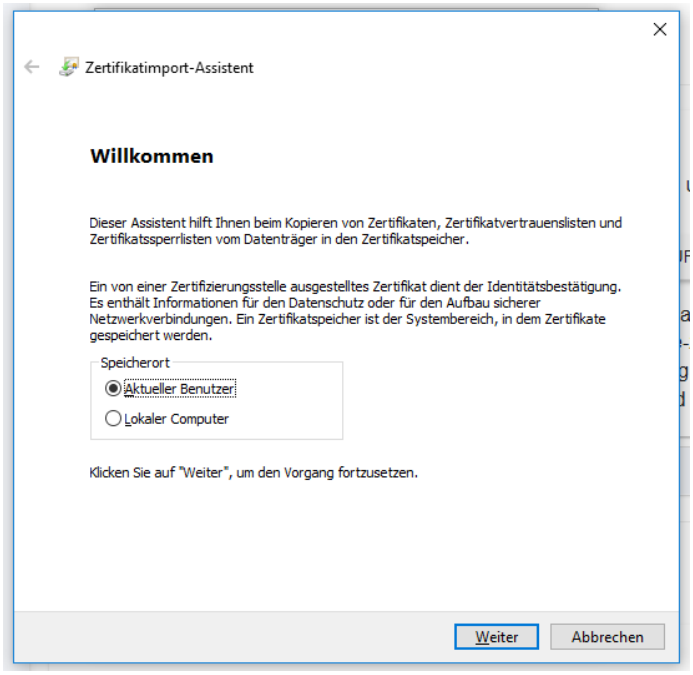
Klicken Sie in dem erscheinenden Dialog erst auf *Speichern* und danach auf *Öffnen.*



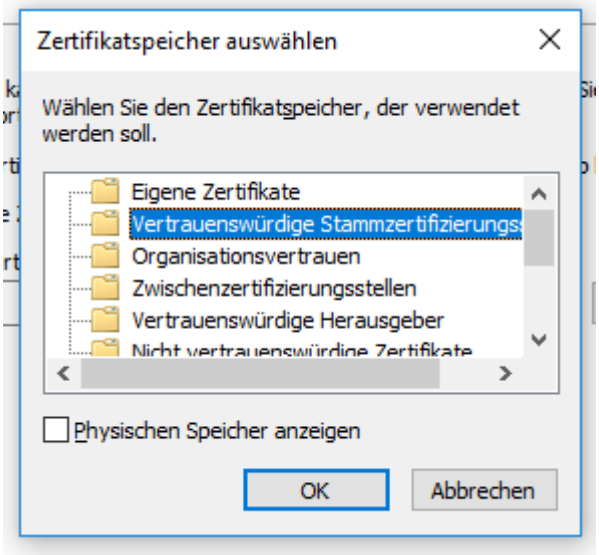
Klicken Sie in dem erscheinenden Fenster auf Zertifikat installieren.



Es öffnet sich der Zertifikatimport-Assistent, den Sie mit *weiter* bestätigen. Klicken Sie jetzt auf *Alle Zertifikate in folgendem Speicher speichern* und klicken Sie anschließend auf *Durchsuchen*.

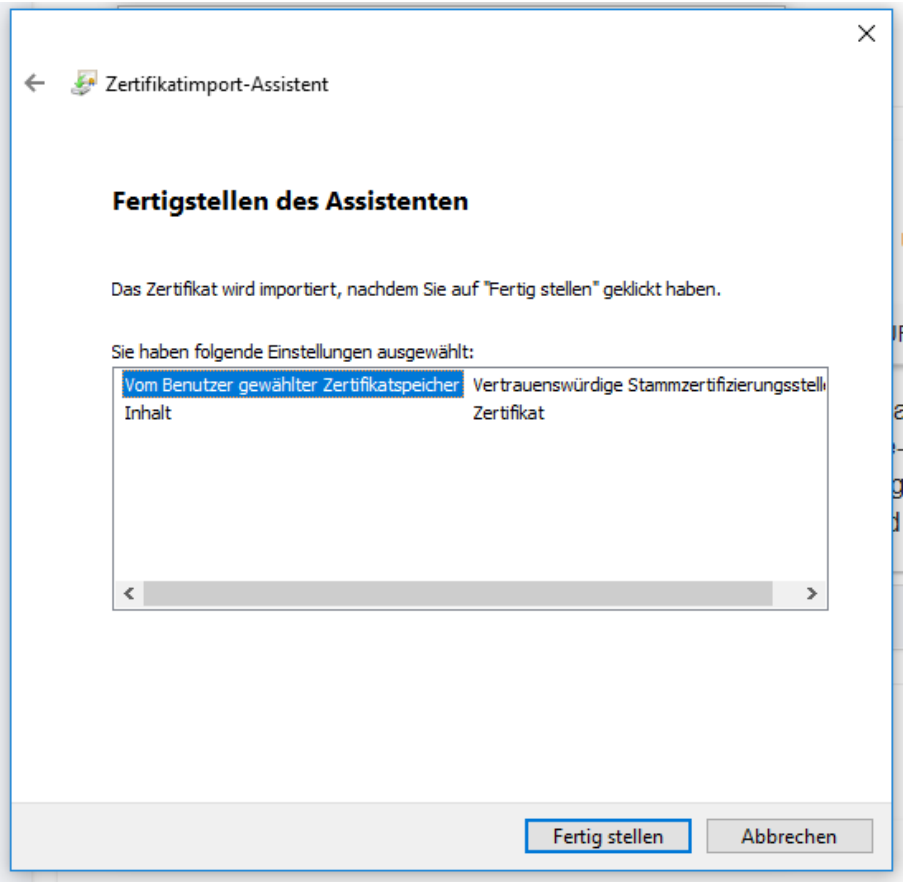


Wählen Sie jetzt den zweiten Eintrag *Vertrauenswürdige Stammzertifizierungsstelle* aus und bestätigen Sie den Vorgang mit *OK*.



Im Zertifikatimport-Assistent klicken Sie auf *Weiter* und anschließend auf *Fertig stellen*.

Bestätigen Sie die folgende Sicherheitswarnung mit *Ja*.



Das eBlocker-Zertifikat ist nun in Windows hinterlegt. Die meisten Browser und Programme können jetzt auf das eBlocker-Zertifikat zugreifen.

Hier eine Auswahl an gängigen Browsern, mit denen Sie die eBlocker Controlbar nun auf HTTPS Seiten sehen können.

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

Für folgende Browser und Programme muss das eBlocker-Zertifikat in dem betreffenden, eigenen Zertifikatsspeicher hinterlegt werden.

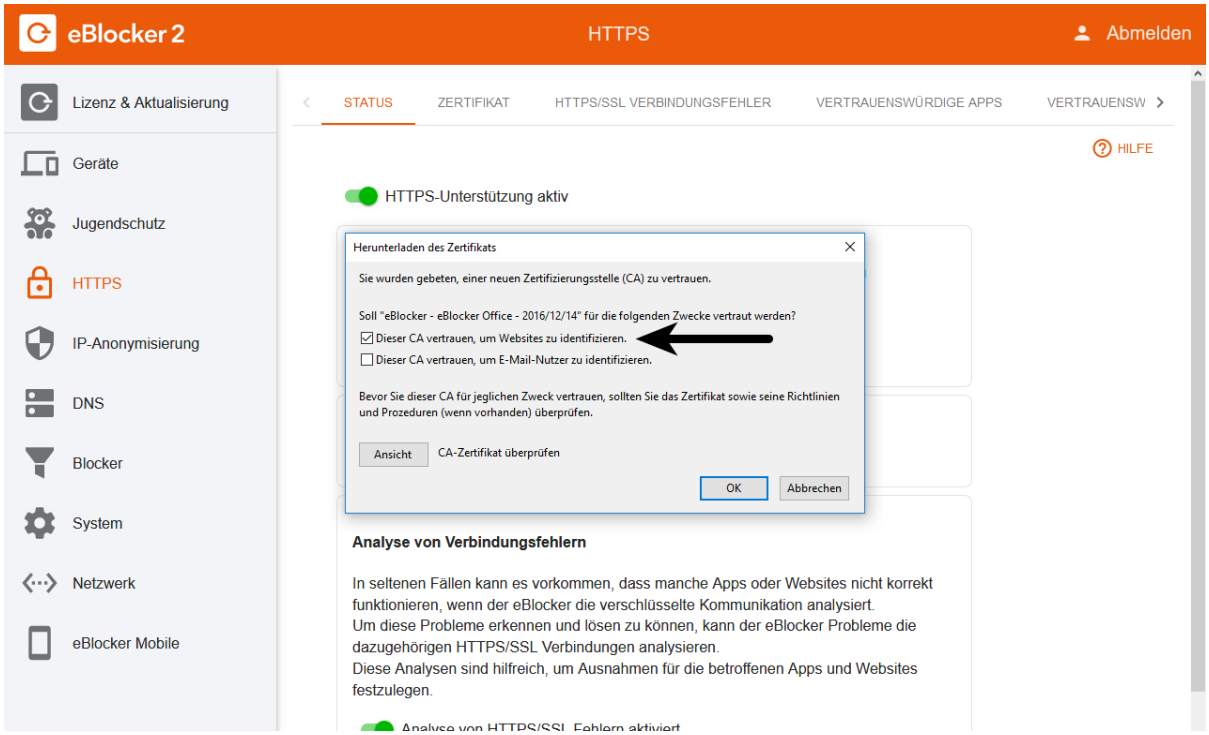
- Firefox
- Cliqz (basiert auf Firefox)
- Seamonkey
- Thunderbird (E-Mail Programm)

Firefox, Cliqz und Seamonkey

Öffnen Sie die eBlocker HTTPS Konfigurationsseite.

Klicken Sie auf den Button *Zertifikat aufnehmen*.

Stellen Sie sicher, dass die erste Checkbox *'Dieser CA vertrauen, um Websites zu identifizieren'* ausgewählt ist (siehe Bilddarstellung).

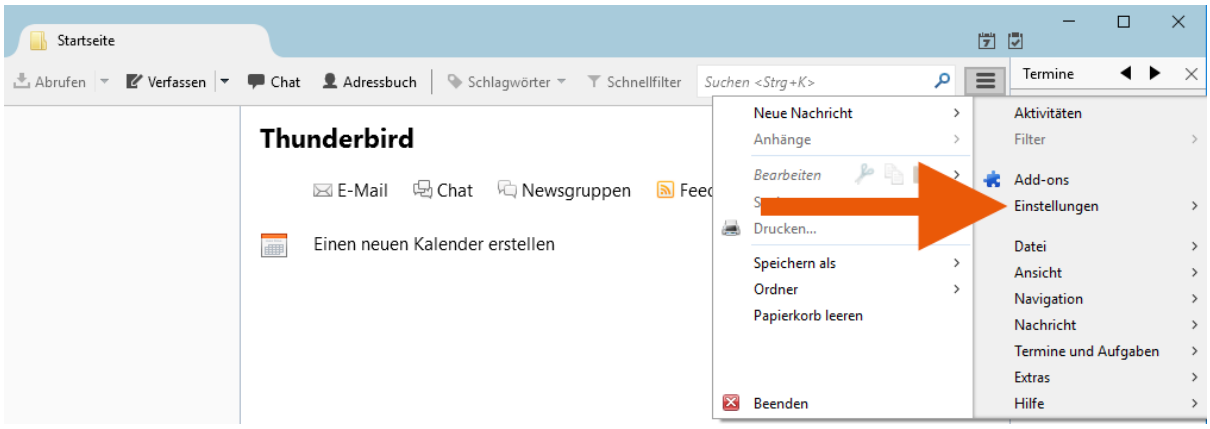


Klicken Sie auf *OK* um das eBlocker-Zertifikat in Firefox aufzunehmen.

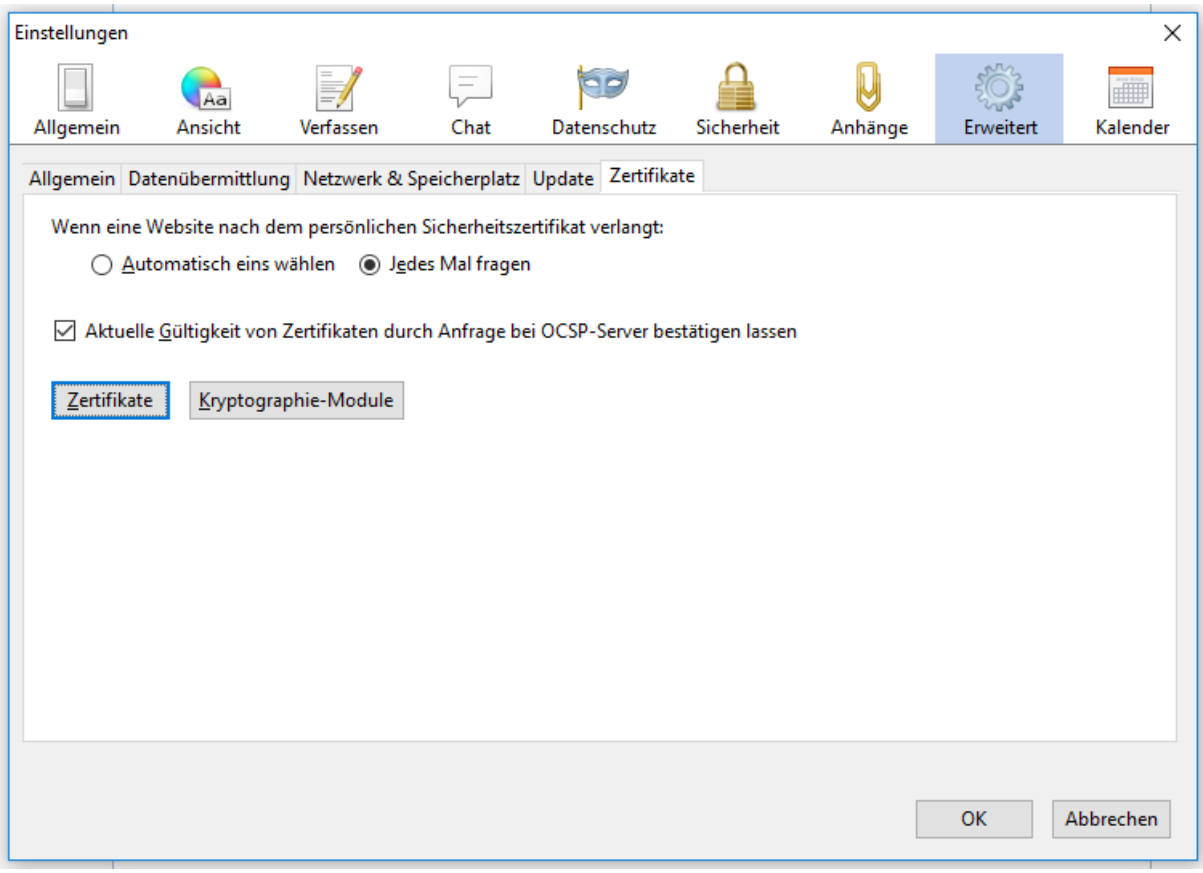
Sie sehen im Firefox, Cliqz oder Seamonkey Browser nun die eBlocker Controlbar auf HTTPS Seiten

Thunderbird (E-Mail Programm)

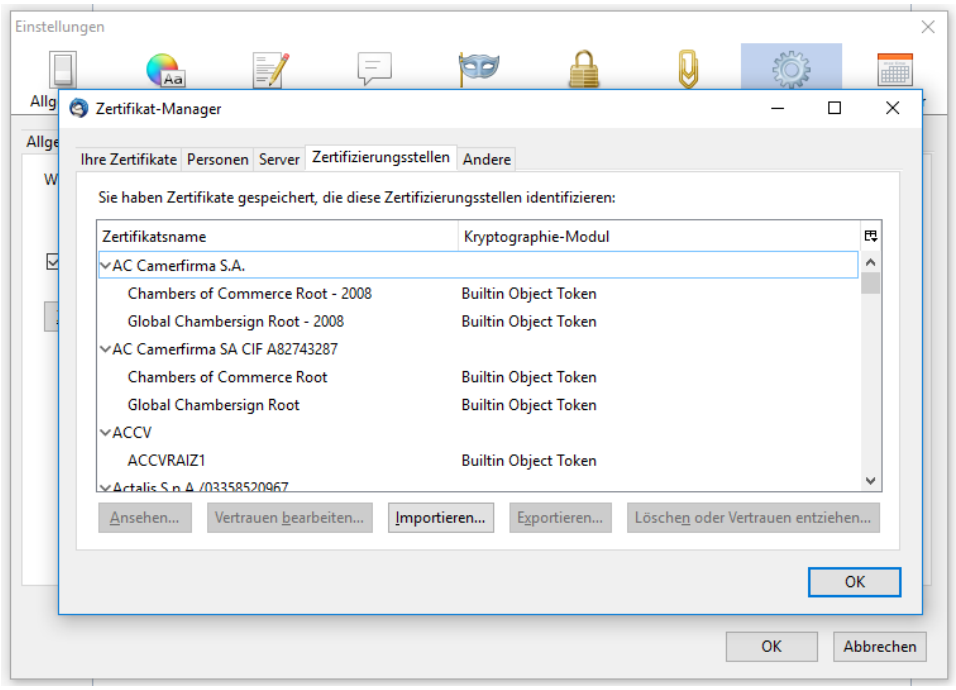
Rufen Sie in Thunderbird das Menü *Einstellungen* auf.



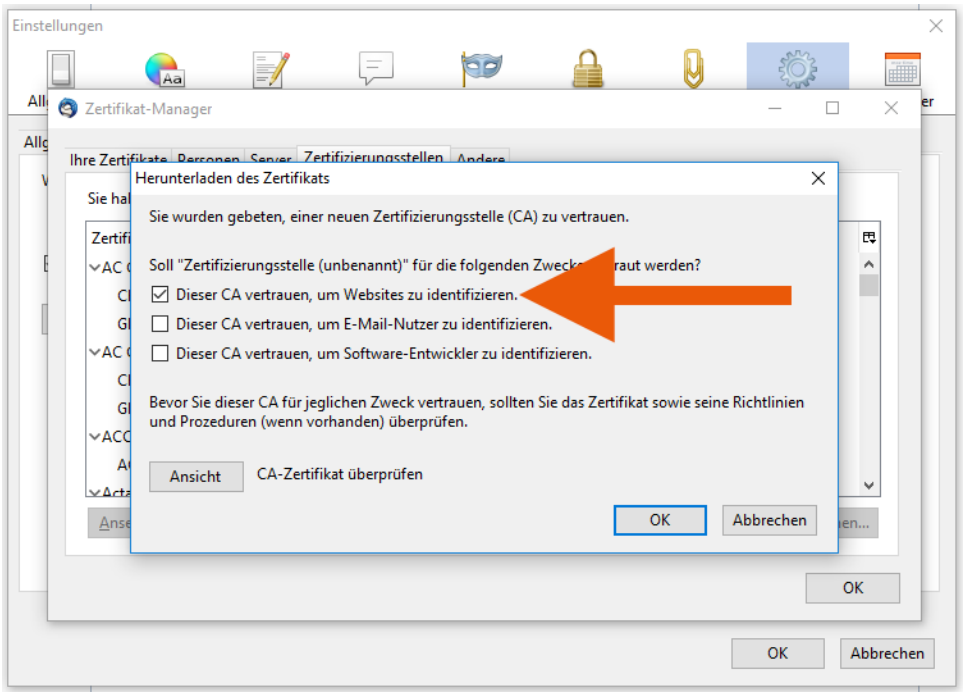
Wählen Sie *Erweitert* aus und klicken Sie bitte auf *Zertifikate*.



Es öffnet sich der Zertifikat-Manager. Dort klicken Sie bitte auf *Importieren* und wählen anschließend das eBlocker Zertifikat aus dem Download Verzeichnis aus.



Laden Sie das eBlocker-Zertifikat mit Öffnen und stellen Sie sicher, dass im folgenden Dialog die erste Checkbox *'Dieser CA vertrauen, um Websites zu identifizieren'* ausgewählt ist und bestätigen Sie mit *OK*.



Klicken Sie nun im Zertifikat-Manager auf *OK* und bestätigen die Einstellungen ebenfalls mit *OK*.

Das Zertifikat ist nun im Thunderbird E-Mail-Programm hinterlegt.

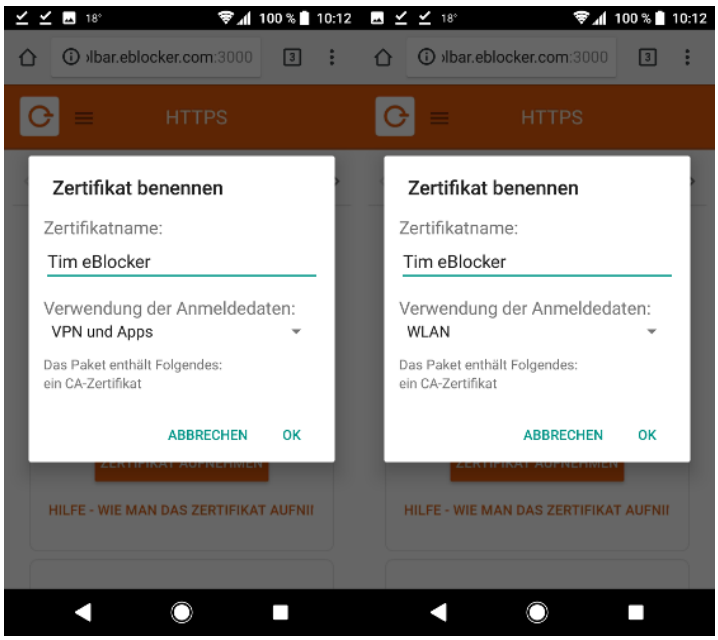
6.2.3 Android

Mit nur wenigen Schritten haben Sie das Zertifikat hinterlegt. Benutzen Sie bitte den Google Chrome Browser.

- Öffnen Sie die eBlocker HTTPS Konfigurationsseite.
- Klicken Sie auf den Button "Zertifikat aufnehmen".
- Geben Sie gegebenenfalls Ihre PIN ein
- Geben Sie dem Zertifikat einen Namen (z.B.: Tim eBlocker).
- Wählen Sie unter Verwendung der Anmeldedaten bitte "VPN und Apps" aus.
- Wiederholen Sie letzten Schritte und speichern Sie das Zertifikat zusätzlich unter "WLAN".

Bei Android Versionen kleiner als Version 6 reicht es, wenn Sie das Zertifikat nur unter "WLAN" speichern.

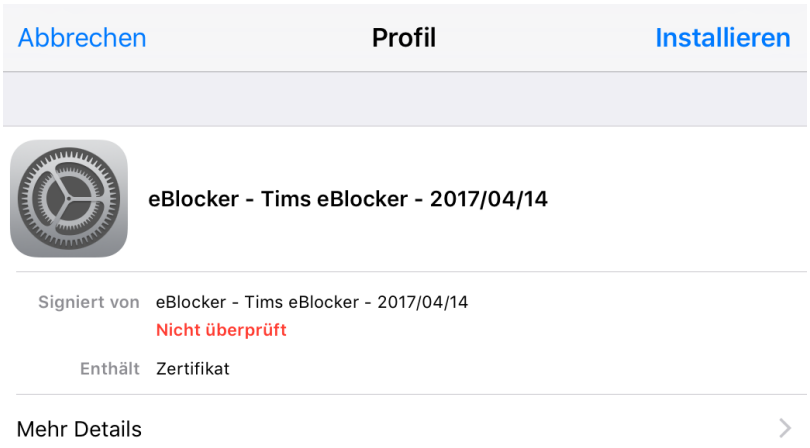
Sie finden das eBlocker Zertifikat im Download Ordner, sollte es nicht automatisch geöffnet werden.

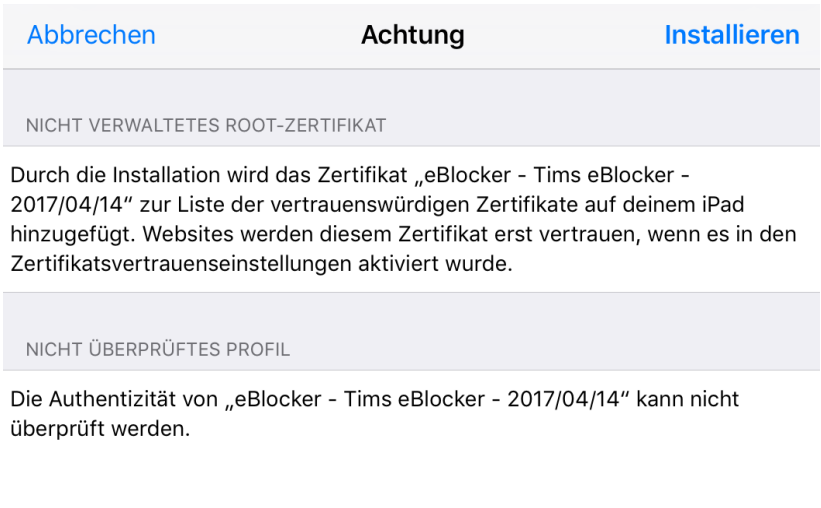


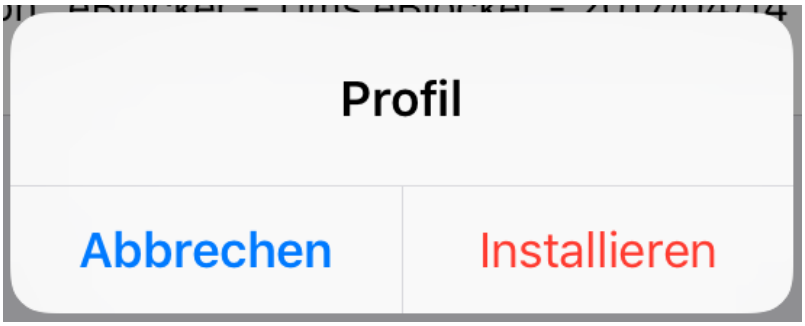
6.2.4 iOS

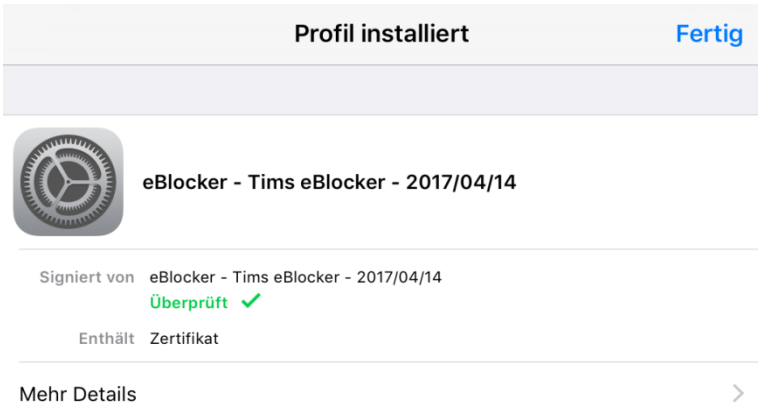
Mit nur wenigen Schritten haben Sie das Zertifikat hinterlegt. Benutzen Sie bitte den iOS Safari Browser.

- Öffnen Sie die eBlocker HTTPS Konfigurationsseite.
- Klicken Sie auf den Button "Zertifikat aufnehmen".
- Es Öffnen sich automatisch die iOS Einstellungen und es wird Ihnen das Profil des eBlocker Zertifikats angezeigt.
- Klicken Sie nun auf "Installieren".
- Im nachfolgenden Dialog klicken Sie nochmals auf "Installieren".
- Bestätigen das Hinterlegen des Zertifikats mit dem Button "Installieren".
- Das eBlocker Zertifikat ist dann in iOS aufgenommen worden.


Abbrechen
Profil
Installieren
eBlocker - Tims eBlocker - 2017/04/14
Signiert von eBlocker - Tims eBlocker - 2017/04/14
Nicht überprüft
Enthält Zertifikat
Mehr Details

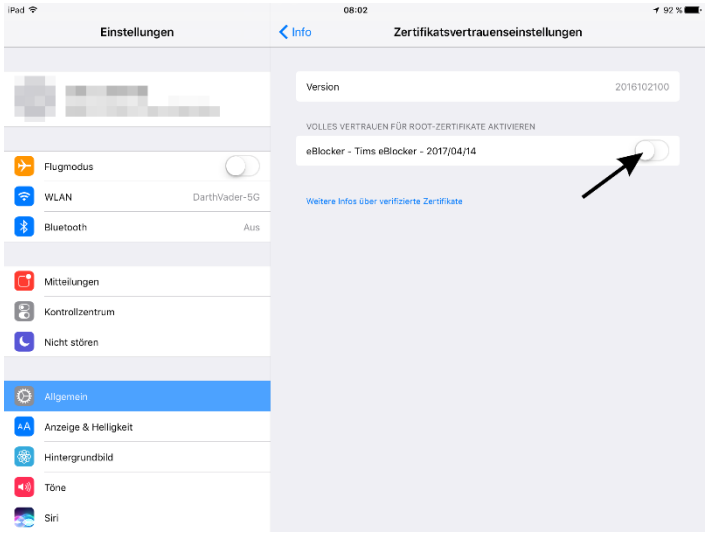

Abbrechen
Achtung
Installieren
NICHT VERWALTETES ROOT-ZERTIFIKAT
Durch die Installation wird das Zertifikat „eBlocker - Tims eBlocker - 2017/04/14“ zur Liste der vertrauenswürdigen Zertifikate auf deinem iPad hinzugefügt. Websites werden diesem Zertifikat erst vertrauen, wenn es in den Zertifikatsvertrauenseinstellungen aktiviert wurde.
NICHT ÜBERPRÜFTES PROFIL
Die Authentizität von „eBlocker - Tims eBlocker - 2017/04/14“ kann nicht überprüft werden.

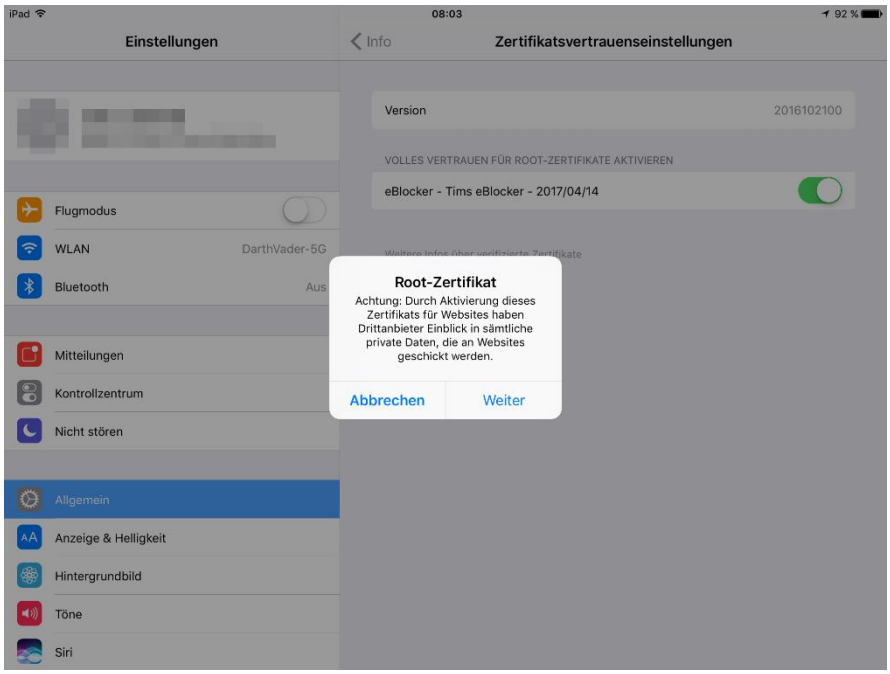

Profil
Abbrechen
Installieren


Profil installiert
Fertig
eBlocker - Tims eBlocker - 2017/04/14
Signiert von eBlocker - Tims eBlocker - 2017/04/14
Überprüft
Enthält Zertifikat
Mehr Details

Ab der iOS Version 10.3 muss das hinterlegte eBlocker Zertifikat noch ein mal aktiviert werden.

- Öffnen Sie die iOS Einstellungen und navigieren zu "Allgemein" > "Info" > "Zertifikatsvertrauenseinstellungen".
- Dort finden Sie das zuvor hinterlegte eBlocker Zertifikat und können es jetzt aktivieren.



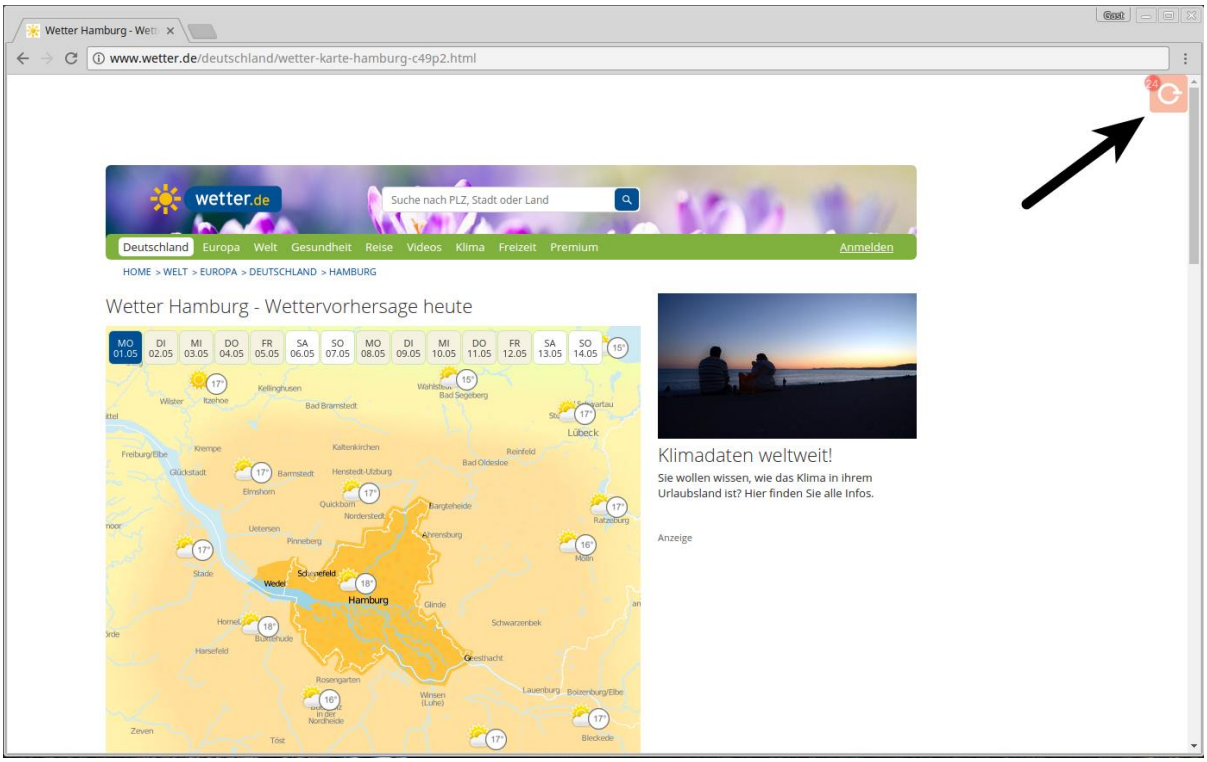


7 Beschreibung der eBlocker Funktionen

Bei der täglichen, normalen Verwendung sollten Sie den eBlocker möglichst gar nicht direkt bemerken. Alles sollte wie gewohnt funktionieren. Viele Webseiten werden sogar schneller geladen, weil aufwändige Werbebanner und –animationen blockiert werden.

7.1 eBlocker Icon

Dass der eBlocker tatsächlich funktioniert und aktiv ist, sehen Sie immer daran, dass auf allen Webseiten rechts oben das eBlocker Icon als durchscheinendes Bild sichtbar ist.



Falls Tracker oder Werbung auf der Seite geblockt wurden, wird zusätzlich die Zahl der insgesamt blockierten Anfragen angezeigt.

Sollten zudem neue Systemnachrichten vorliegen, wird ein kleines Ausrufungszeichen eingeblendet.

Durch Klick auf das eBlocker Icon öffnen Sie die sogenannte Controlbar.

7.2 eBlocker Controlbar Base, Pro, Family

Über die Controlbar haben Sie schnellen Zugriff auf wichtige Funktionen zur aktuell geladenen Seite oder zu Ihren verwendeten Geräten.

eBlocker Base

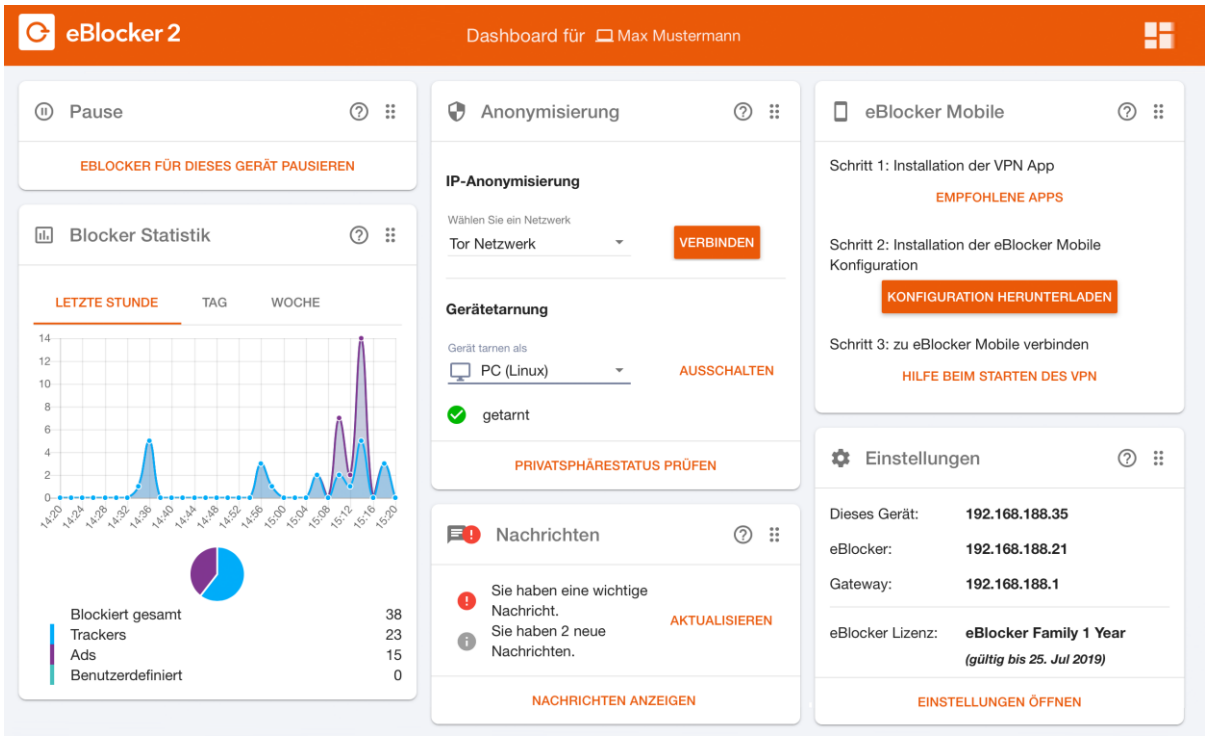
eBlocker Pro

eBlocker Family

Die Funktionen der Controlbar werden in den folgenden Abschnitten ausführlich beschrieben.

7.3 Dashboard

Die Übersicht - auch als Dashboard bekannt, bietet Ihnen den gleichen Funktionsumfang wie die eBlocker Controlbar. Zusätzlich bietet er auch einen schnellen Zugang zu den Einstellungen Ihres eBlockers.



Tipp: Setzen Sie in Ihrem Browser ein Lesezeichen für das eBlocker Dashbard, oder legen Sie sich das eBlocker Dashboard als Startseite an. Für mehr Information zum eBlocker Dashboard, lesen Sie unseren Artikel „Tipps zu dem eBlocker Dashboard“ in unserem Forum unter der Wissensdatenbank.

Es gibt in dem Dashboard folgende Menüs, welche Sie mit der Maus nach Ihren Belieben anordnen können.

Pause

Hier können Sie Ihren eBlocker für dieses Gerät pausieren. Die Pause wird für 5 Minuten gestartet, kann aber jeder Zeit für weitere 5 Minuten verlängert, oder verkürzt werden.

Einstellungen

Hier sehen Sie die IP-Adressen Ihres Gerätes, von Ihrem eBlocker und von Ihrem Gateway (Router). Zusätzlich sehen Sie hier auch Ihre eBlocker Lizenz und können die eBlocker Einstellungen öffnen.

Nachrichten

In bestimmten Fällen kann Ihnen Ihr eBlocker Nachrichten senden. Diese können Sie sich hier anzeigen lassen.

Conrolbar

Hier können Sie bestimmen ob und wo (links und rechts) das eBlocker Symbol im Browser angezeigt werden soll. Sie können das eBlocker Symbol zum Beispiel auch nur auch 5 Sekunden lang anzeigen lassen. Mit der Einstellungen „Nur im Standard-Browsern“ soll verhindert werden, dass Sie das eBlocker Symbol auch gegebenenfalls in Apps sehen.

HTTPS-Unterstützung (nur eBlocker Pro und eBlocker Family)

Hier können Sie die HTTPS Unterstützung für Ihr Gerät aktivieren und auch das eBlocker Zertifikat herunterladen. Zusätzlich überprüft dieses Menü auch, ob das eBlocker Zertifikat richtig hinterlegt wurde.

Anonymisierung (nur eBlocker Pro und eBlocker Family)

Hier können Sie auswählen, ob Sie über das Tor-Netzwerk, oder über eine VPN-Verbindung surfen wollen.

Sofern die HTTPS Funktion des eBlocker aktiviert ist, könne Sie in diesem Menü auch die Gerätetarnung aktivieren.

Zusätzlich habe Sie hier die Möglichkeit Ihren Privatsphärenstatus zu testen. Dazu haben wir für Sie eine spezielle Webseite erstellt.

Blocker Statistik (nur eBlocker Pro und eBlocker Family)

Hier können Sie die Statistik der geblockten Inhalte für die letzte Stunde, den letzten Tag, oder der letzten Woche einsehen.

Blocker Statistik (Gesamt) (nur eBlocker Pro und eBlocker Family)

Hier können Sie eine genauere Statistik der geblockten Inhalte seit dem letzten Start des eBlockers sehen.

Die Top 25 Domains für die Tracker und die Werbung werden separat angezeigt.

Tracker und Ad Blockerregeln (nur eBlocker Pro und eBlocker Family)

Hier können Sie festlegen, ob der eBlocker alle Verbindungen zu Trackern oder zu Werbung blockieren soll. Sind diese beiden Einstellungen deaktiviert, wird Ihr eBlocker auch keine Tracker und Werbung blockieren.

Sie können gegebenenfalls auch bestimmte Verbindungen zu einer Domain in einer Whiteliste für dieses Gerät erlauben, oder in einer Blacklist auch zusätzliche Domains für ein Gerät blockieren.

eBlocker Mobile

Hier können Sie für Ihr Gerät die OpenVPN Konfiguration für die eBlocker Mobile Funktion herunterladen. Wenn die eBlocker Mobile Funktion nicht aktiviert ist, werden Sie dieses Menü auch nicht sehen können.

Benutzer (nur eBlocker Family)

Sofern Ihr Gerät einem Benutzer zugeordnet ist, kann dieses Menü angezeigt werden.

Hier können Sie zum Beispiel das Gerät eines Benutzers übernehmen, die PIN für dieses Gerät ändern, oder das Gerät sperren.

7.4 Tracker und Werbung (Tracker- und Ad-Blocker)

Gültig für **eBlocker Pro** und **eBlocker Family**

Eine der zentralen und wichtigsten Funktionen des eBlockers ist zu verhindern, dass Dritte Ihr Surfverhalten überwachen und so ein detailliertes Persönlichkeitsprofil von Ihnen erstellen.

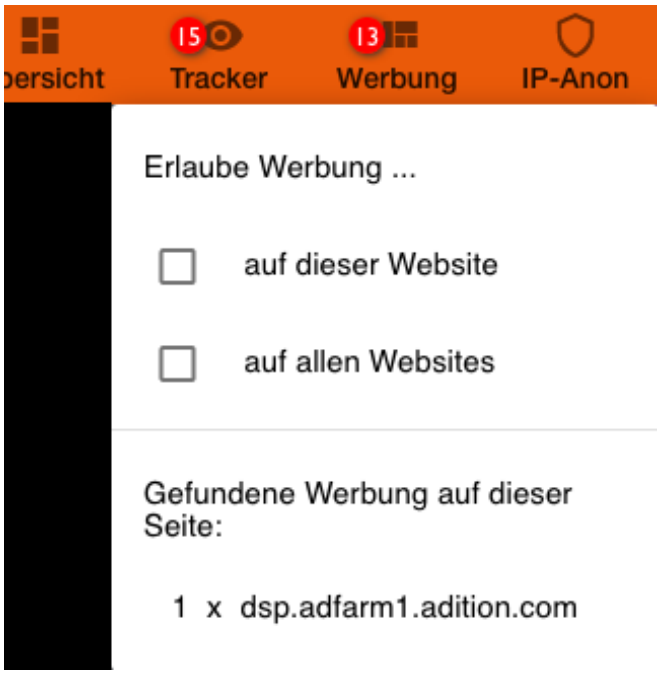
Um das zu erreichen, blockiert der eBlocker standardmäßig die Datenübermittlung an Datensammler und verhindert das Laden von Werbeeinblendungen aus Werbenetzwerken, die ebenfalls Ihr Surfverhalten protokollieren und zu Profilen verdichten.

In der Controlbar können Sie auf jeder Seite sehen, wie viele Verbindungen zu Datensammlern und Werbenetzwerken jeweils verhindert wurden. Mit einem Klick auf das Symbol "Tracker" und "Werbung", können Sie sehen, wie viele Tracker und Werbung in den letzten 60 Sekunden und 10 Minuten blockiert wurden. Sie sehen dort auch eine Auflistung aller blockierten Verbindungen.

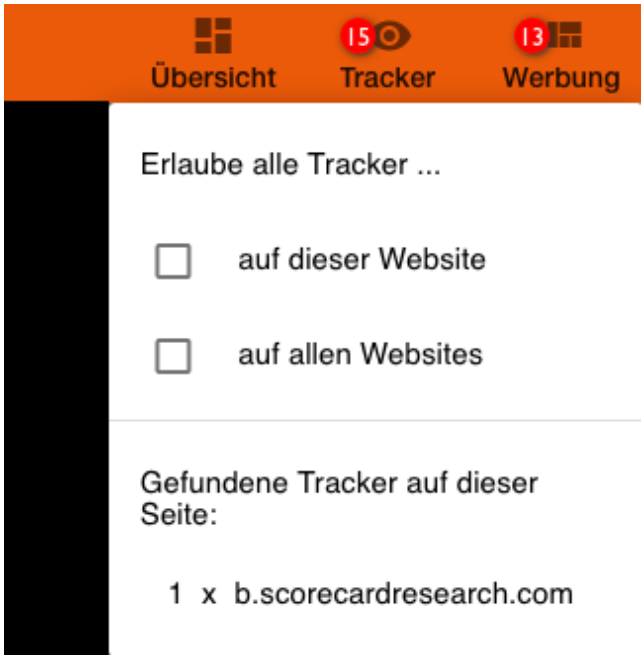
eBlocker will Ihre Privatsphäre schützen, aber eBlocker versucht nicht eventuelle Content-Sperren der Verlage zu umgehen. Webseiten, wie zum Beispiel bild.de erkennen, dass der eBlocker auch Werbung blockiert und stellt die gewünschten Inhalte dann ggf. nicht mehr kostenlos zur Verfügung.

Mit einem Klick auf "Werbung" in der Controlbar, können Sie das eBlocker Modul zur Filterung von Werbung entweder global oder individuell für diese Seite deaktivieren und bekommen in der Regel Zugriff auf die Inhalte. Genauso einfach können Sie die Filterung wieder aktivieren. Der Tracker-Blocker ist dann nach wie vor aktiv, so dass Sie weiterhin vor Trackern geschützt bleiben.

Aber Vorsicht: Auch wenn der Tracker-Blocker aktiv ist, erfasst Werbung Ihr Persönlichkeitsprofil.



Genauso wie das Modul zur Filterung von Werbung, lässt sich das Modul zur Filterung von Trackern global oder individuell für eine Webseite deaktivieren oder aktivieren.



Seiten für die Sie die Werbung oder Tracker, zugelassen haben, werden in der eBlocker Übersicht (Dashboard) in einer Karte aufgelistet. Auch dort können Sie für die gewünschte Seite die Anzeige der Werbung und Tracker zulassen oder wieder unterbinden.

7.5 Anon (IP-Anonymisierung)

Immer wenn Sie im Internet unterwegs sind, übermitteln Sie der angesprochenen Webseite Ihre sogenannte IP-Adresse. Das ist so ähnlich wie die Nummernübertragung beim Telefon. Es gibt zwar kein öffentliches „Telefonbuch“ für IP-Adressen, aber Ihr Internet-Provider weiß, wer, wann und welche IP-Adresse verwendet hat. Diese Daten werden – Stichwort „Vorratsdatenspeicherung“ – eine Zeitlang gespeichert und ggf. an staatliche Behörden herausgegeben.

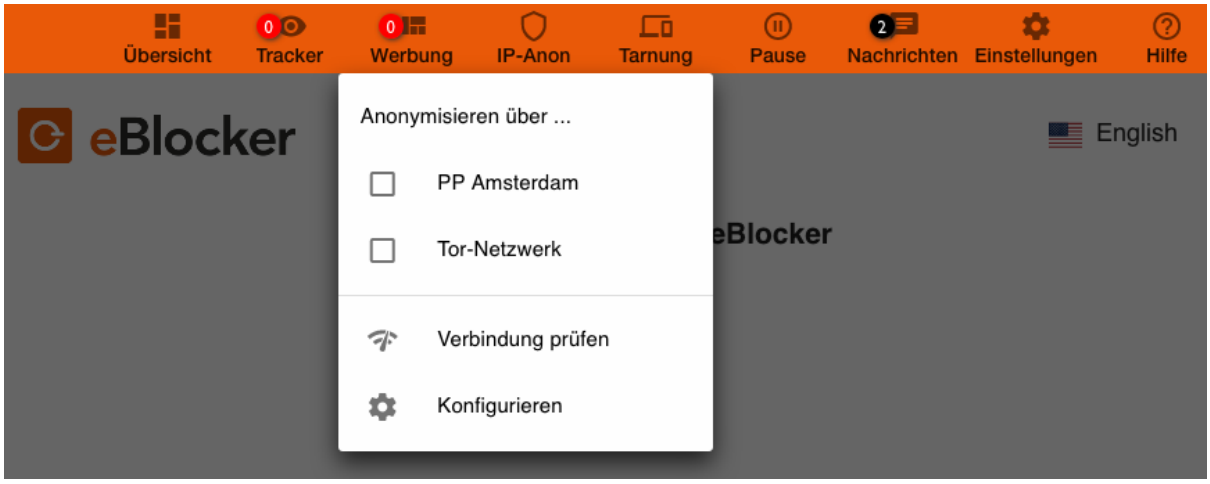
Ganz unabhängig davon, kann jede IP-Adresse dem Provider und auch einer geografischen Region zugeordnet werden. So weiß die angesprochene Webseite, woher Sie kommen.

Zur Verschleierung der eigenen IP-Adresse, d.h. um zusätzliche Anonymität im Internet zu erreichen, können Sie die IP-Anonymisierung aktivieren.

Sobald die „IP-Anonymisierung“ eingeschaltet ist, werden sämtliche HTTP-Anfragen durch ein Anonymisierungsnetzwerk geleitet. Ist SSL/HTTPS auf dem eBlocker aktiviert, werden auch HTTPS-Anfragen anonymisiert. Ab sofort bieten wir neben dem Tor-Netzwerk auch alternative Netzwerke an, die das OpenVPN-Protokoll unterstützen.

Wie Sie das Tor-Netzwerk einrichten und nutzen, lesen Sie in Kapitel 8.5.

Wie Sie andere Netzwerke einrichten und nutzen, lesen Sie in Kapitel 8.5.2.



Mit „Verbindung prüfen“ können Sie hier überprüfen, ob eine Verbindung über ein Tor Anonymisierungsnetzwerk besteht, bzw. welche Daten von außen sichtbar sind.

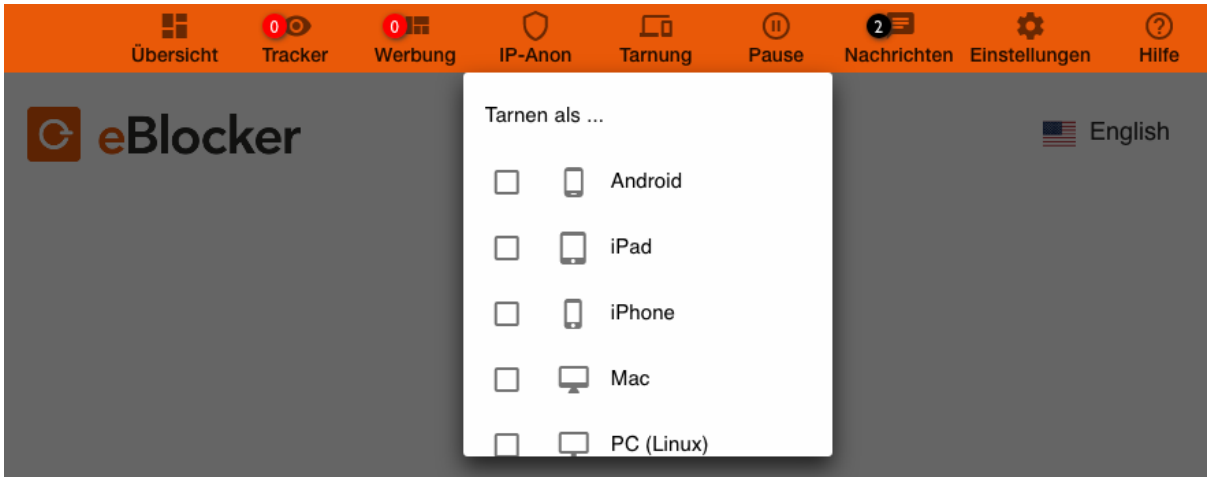
Mit "Konfigurieren" gelangen Sie direkt zu den Einstellungen "IP-Anonymisierung".

7.6 Tarnung

Gültig für **eBlocker Pro** und **eBlocker Family**

Jeder Browser identifiziert sich im Internet bei der aufgerufenen Webseite mit der sogenannten „User Agent“-Kennung. Diese Kennung liefert der Webseite genaue Angaben zum verwendeten Endgerät, Betriebssystem und Browser. Sie wird nicht nur verwendet, um Sie zu identifizieren und um ein Persönlichkeitsprofil zu erstellen. Sie wird auch häufig von Shops verwendet, um individuelle Preise anzubieten. So kann es beispielsweise vorkommen, dass Sie bei Verwendung eines Tablets einen anderen Preis für dasselbe Produkt erhalten, als von einem stationären PC.

Mit Hilfe der Gerätetarnung des eBlockers, können Sie Ihr Endgerät tarnen und veranlassen, dass die User-Agent-Kennung eines anderen Gerätetyps gesendet wird. So können Sie den Schutz Ihrer Privatsphäre weiter verbessern und im Idealfall die dynamische Preisgestaltung einiger Shops zu Ihrem Vorteil gestalten.



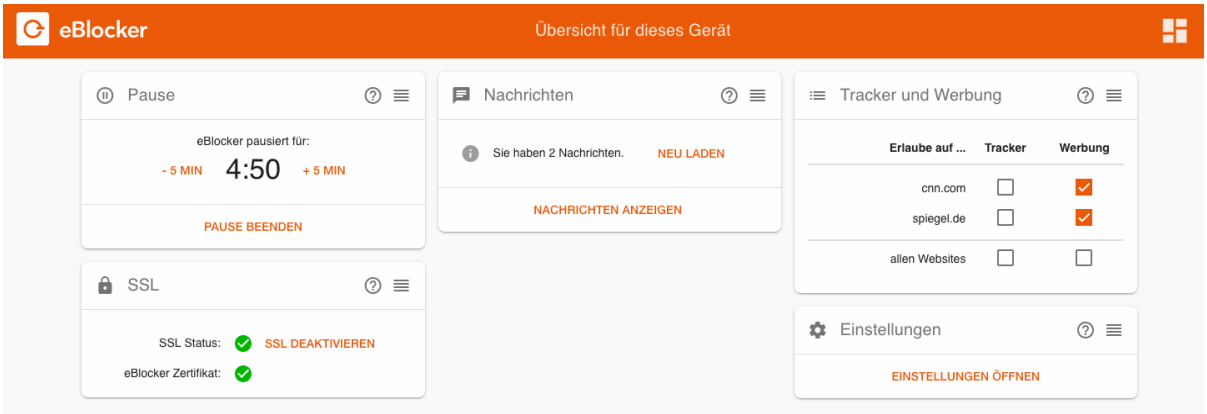
Öffnen Sie hierfür die Controlbar. Gehen Sie auf "Tarnung" und tarnen Sie Ihr Gerät beliebig mit einem Klick auf das gewünschte Gerät.

7.7 Pause

Gültig für **eBlocker Base**, **eBlocker Pro** und **eBlocker Family**

Mit „Pause“ deaktivieren Sie den eBlocker für das aktuelle Gerät, mit dem Sie gerade im Internet surfen.

Die eBlocker Übersicht (auch Dashboard genannt) öffnet sich in einem neuen Browser-Tab, sobald Sie in der eBlocker Controlbar auf „Pause“ klicken. In dem Übersicht können Sie die Pause bequem um 5 Minuten verlängern, verkürzen, die Pause beenden, oder die eBlocker Einstellungen aufrufen.



7.8 Einstellungen

Klicken Sie auf „Einstellungen“, um Ihren eBlocker individuell einzustellen. Alle Einstellungsmöglichkeiten des eBlockers sind im Kapitel 8 ausführlich beschrieben.

7.9 Hilfe

Bei Fragen und Problemen können Sie hier auf dieses Benutzerhandbuch zurückgreifen. Darüber hinaus haben wir ein Forum für technische Fragen eingerichtet, in dem Sie viele Antworten auf die gängigsten Fragen finden: http://forum.eBlocker.com

Zudem beantworten wir Ihre Fragen auch gerne per E-Mail (siehe Anhang Anhang D).

8 Die Einstellungsmöglichkeiten des eBlockers

Die wichtigsten Funktionen des eBlockers, die Sie für das normale, tägliche Arbeiten im Internet brauchen, finden Sie über das eBlocker Icon (rechts oben auf allen Internetseiten) und über die Controlbar (siehe Abschnitt 7).

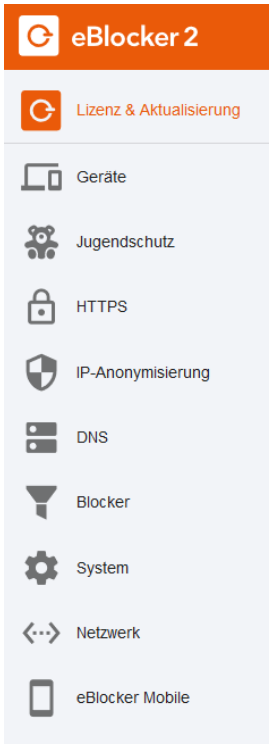
Einige Einstellungen können aber einfacher oder ausschließlich über die sogenannte Konsole getätigt werden.

Die Einstellungskonsole des eBlockers erreichen Sie über die Controlbar (siehe **Fehler! Verweisquelle onnte nicht gefunden werden.**) über das Icon „Einstellungen“.

Die Funktionen der Einstellungskonsole sind in die folgenden Bereiche untergliedert:

Menü	**Verfügbar für:**
Lizenz & Aktualisierung	eBlocker Base, eBlocker Pro und eBlocker Family
Geräte	eBlocker Base, eBlocker Pro und eBlocker Family
HTTPS	eBlocker Pro und eBlocker Family
IP-Anonymisierung	eBlocker Base, eBlocker Pro und eBlocker Family
DNS	eBlocker Base, eBlocker Pro und eBlocker Family
Blocker	eBlocker Pro und eBlocker Family
System	eBlocker Base, eBlocker Pro und eBlocker Family
Netzwerk	eBlocker Base, eBlocker Pro und eBlocker Family
eBlocker Mobile	eBlocker Base, eBlocker Pro und eBlocker Family

Den jeweiligen Bereich erreichen Sie durch Klick auf den entsprechenden Link im Seitenregister auf der linken Seite.



Eine detaillierte Beschreibung aller Bereiche finden Sie in den folgenden Abschnitten.

Beim erstmaligen Aufruf der Einstellungskonsole, bzw. solange Sie die Aktualisierungslizenz noch nicht auf dem Gerät aktiviert haben, startet automatisch der Aktivierungsassistent, der Sie durch die Aktivierung begleitet.

8.1 Allgemein

Allgemeine Einstellungen und Informationen zu Ihrem eBlocker.

Diese Seite ist weiter unterteilt in die folgenden Abschnitte:

- Lizenz
- Aktualisierung
- Admin-Passwort
- Über eBlocker

8.1.1 Lizenz

Hier sehen Sie Details zu Ihrer Aktualisierungslizenz und Ihrem eBlocker.

Über die Schaltfläche „Lizenz aktivieren“ können Sie den Lizenzschlüssel für eine Verlängerung der Lizenz (z.B. auf eine „Lifetime“-Lizenz) oder für ein Upgrade der Lizenz (z.B. von eBlocker Pro auf eBlocker Family) eingeben und aktivieren. Der Link „Lizenz kaufen“ führt Sie in den eBlocker Online Shop. Der Link „Lizenz übertragen (von Gerät zu Gerät)“ führt Sie auf eine Webseite, über die Sie die Lizenz von einem Gerät lösen können, um sie anschließend für ein anderes Gerät zu verwenden.

8.1.2 Aktualisierung

Diese Seite zeigt an, welche Versionen der eBlocker Software sowie der eBlocker Filterregeln gerade auf Ihrem Gerät in Betrieb sind.

Falls eine gültige Aktualisierungslizenz für das Gerät aktiviert ist, können Sie automatische Aktualisierungen einschalten und festlegen, zu welcher Uhrzeit diese täglich durchgeführt werden sollen.

In der Grundeinstellung sind automatische Aktualisierungen eingeschaltet und werden in der Zeit zwischen 02:00 Uhr und 03:00 Uhr Ortszeit durchgeführt.

Wenn Sie die Funktion der automatischen Aktualisierungen deaktivieren, können Sie jederzeit selber Updates einspielen. Sobald ein neues Update für Sie zur Verfügung steht, wird dies neben dem Button "auf Aktualisierungen prüfen" angezeigt.

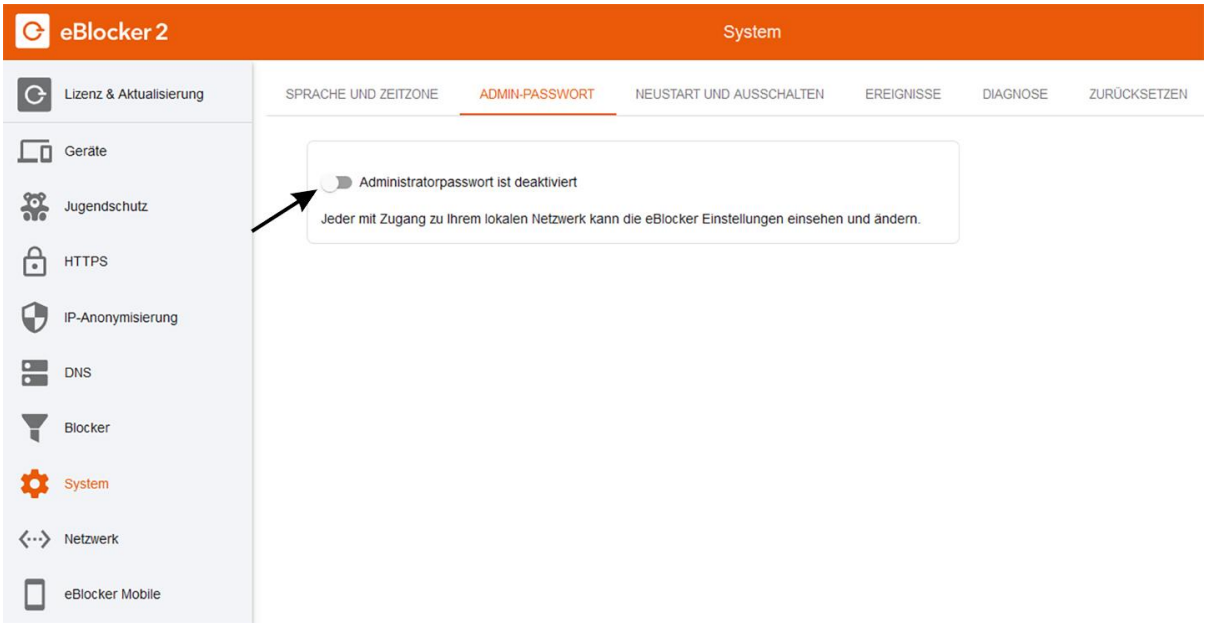
8.1.3 Admin-Passwort

In der Grundeinstellung ist die eBlocker-Konsole für jeden Benutzer im lokalen Netzwerk erreichbar. Das ist in vielen Fällen praktisch und ausreichend.

Wir empfehlen jedoch, ein Administratorpasswort zu vergeben, so dass wichtige Einstellungen und Informationen des eBlockers nur nach Eingabe dieses Passworts erreichbar sind.

Sobald ein Passwort vergeben wurde, kann die eBlocker-Konsole nur durch Eingabe dieses Passworts geöffnet werden.

Bitte bewahren Sie das Administratorpasswort gut auf! Falls Sie es doch einmal vergessen haben sollten, können Sie es zurücksetzen indem Sie auf den Schiebeschalter neben der Beschriftung „Administratorpasswort ist deaktiviert“ anklicken.



8.1.4 Über eBlocker

Hier finden Sie einige allgemeine und rechtliche Angaben bzw. Hinweise zum eBlocker sowie Informationen, wie Sie unser Supportforum erreichen (siehe Anhang D).

8.2 Jugendschutz

Gültig für **eBlocker Family**

Wenn Sie die Jugendschutz-Funktionen bereits in früheren Versionen verwendet haben, beachten Sie bitte die Hinweise in Abschnitt 8.2.19.

8.2.1 Jugendschutz aktivieren

Um den Jugendschutz zu verwenden, vergeben Sie zunächst ein Passwort für den Administrator. Niemand außer dem Administrator kann dann zu den eBlocker-Einstellungen gelangen und die Jugendschutz-Einstellungen ändern oder deaktivieren.

Das Administrator-Passwort vergeben Sie in den „eBlocker Einstellungen > System" unter „Admin-Passwort".

Navigieren Sie in das Menü „eBlocker Einstellungen > Jugendschutz". Der Bereich „Jugendschutz“ stellt vier Unterseiten bereit, deren Funktion im Folgenden ausführlich erläutert wird:

- Benutzer
- Jugendschutz-Profile
- Erlaubte Websites
- Verbotene Websites

8.2.2 Benutzer und Jugendschutz-Profile

Um den Jugendschutz für einzelne Geräte in Ihrem Heimnetz zu aktivieren, müssen zunächst alle zu schützenden Geräte einem Benutzer zugewiesen werden. Über diesen Benutzer ergibt sich das jeweils aktive Jugendschutz-Profil, wodurch der Zugriff auf bestimmte Websites oder zu bestimmten Zeiten eingeschränkt werden kann.

Neu in Version 1.3 ist, dass der aktive Benutzer eines Gerätes – und damit das aktive Schutzprofil – jederzeit durch Eingabe einer Benutzer-PIN gewechselt werden kann. So dass eine flexible Nutzung der Geräte möglich ist.

Beispiel 1:

Das Familien-Tablet ist jedem Familien-Mitglied zugänglich, auch die Kinder können es jederzeit ohne Beaufsichtigung verwenden. Daher sollte das Tablet einem Benutzer mit eingeschränktem Jugendschutz-Profil zugeweisen werden, um den größtmöglichen Schutz bei unbeaufsichtigter Verwendung zu gewährleisten. Wenn nun ein Erwachsener das Tablet verwenden will, kann die Jugendschutz-Funktion durch Wechsel des Benutzers vorübergehend aufgehoben werden. Für den Benutzerwechsel muss eine PIN eingegeben werden. Nach Verwendung durch den Erwachsenen sollte der Benutzer zurückgesetzt werden oder der Internet-Zugang für das Gerät ganz gesperrt werden.

Beispiel 2:

Das Smartphone eines Elternteils befindet sich immer in Besitz dieses Elternteils. Es ist zudem systemseitig mit einer PIN gegen unberechtigte Verwendung geschützt. Die Kinder können dieses Smartphone also niemals unbeaufsichtigt verwenden. In diesem Fall ist es unnötig, dem Gerät einen expliziten Benutzer oder ein Jugendschutz-Profil zuzuweisen.

8.2.3 Drei einfache Schritte

Folgende Schritte müssen ausgeführt werden, um die Jugendschutz-Funktionen für Ihr Heimnetz zu aktivieren:

- Legen Sie für alle Familienmitglieder einen eBlocker-Benutzer an (s. Abschnitt 8.2.4).
- Weisen Sie jedem Benutzer das passende Jugendschutz-Profil zu. Der eBlocker stellt Beispielprofile bereit, die Sie an Ihre Bedürfnisse anpassen können. Oder Sie legen selbst weitere Jugendschutz-Profile an (s. Abschnitt 8.2.7).
- Weisen Sie allen Geräten, die durch die Jugendschutz-Funktionen geschützt werden sollen, einen Hauptbenutzer zu (s. Abschnitt 8.2.11). Es ist jederzeit möglich den aktiven Benutzer eines Gerätes durch Eingabe einer individuellen Benutzer-PIN zu wechseln (s. Abschnitt 8.2.18).

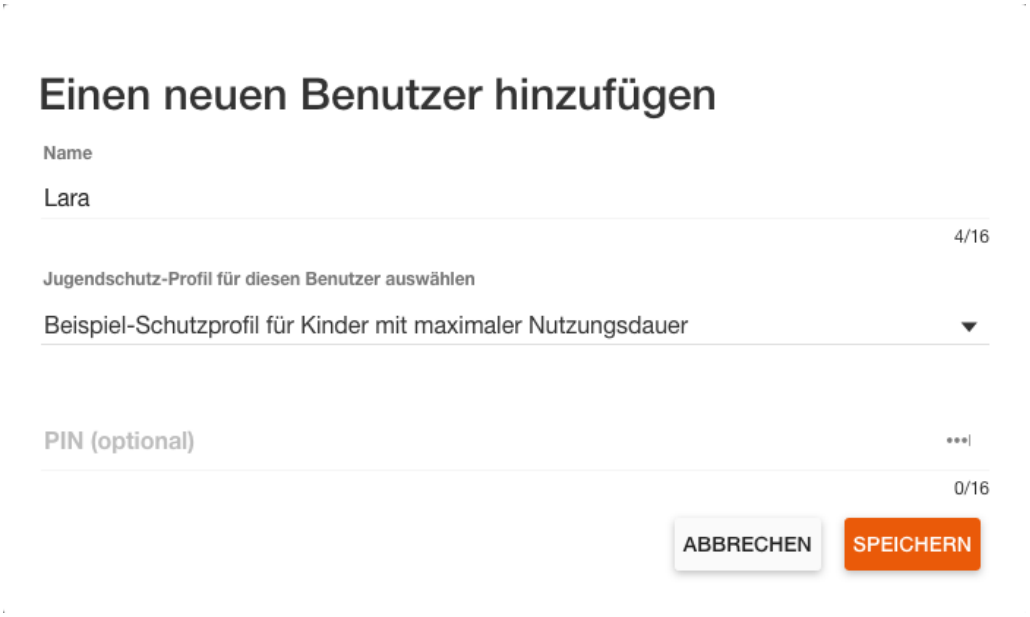
8.2.4 Neuen Benutzer anlegen

Navigieren Sie in das Menü „eBlocker Einstellungen > Jugendschutz" und wählen Sie dort die Seite „Benutzer“:

Wenn Sie die Jugendschutz-Funktionen noch nicht verwendet haben, ist die Liste der Benutzer noch leer. Nachdem Sie einige Benutzer eingerichtet haben, sieht die Seite etwa so aus:

Um einen neuen Benutzer anzulegen, klicken Sie auf „Neuer Benutzer“. Es öffnet sich ein Dialogfenster (s.u.). Geben Sie dort einen Namen ein und wählen Sie ein Jugendschutz-Profil aus.

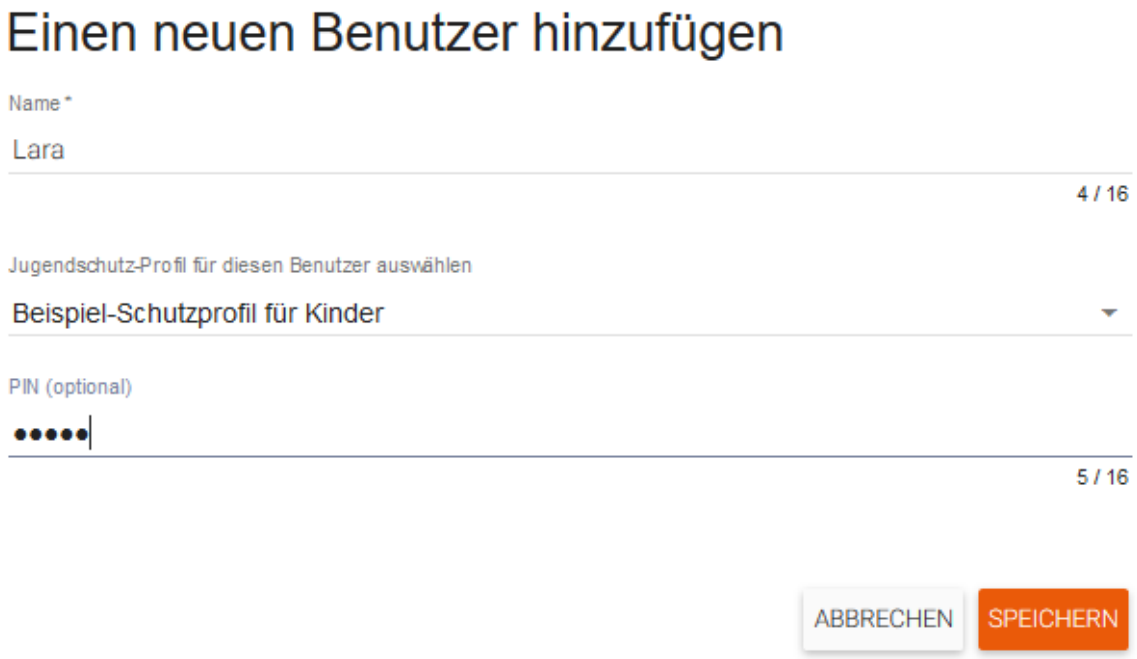
Zusätzlich sollten Sie eine PIN für alle Benutzer vergeben, die ein anderes Gerät übernehmen dürfen. Vergeben Sie z.B. eine PIN für alle Erwachsenen und die älteren Kinder.



Beachten Sie, dass jeder Benutzer, der eine PIN erhalten hat, die eigene PIN selbst ändern kann (s. Abschnitt 8.2.18). Ebenso können sie alle anderen Einstellungen jederzeit einsehen und ändern.

8.2.5 Einstellungen zu einem Benutzer ändern

Klicken Sie dazu auf den Name eines Benutzers. Die aktuellen Einstellungen und Details zu diesem Benutzer werden dann sichtbar:



Sie können den Namen des Benutzers ändern, ein anderes Jugendschutz-Profil für den Benutzer auswählen und festlegen, ob der Benutzer andere Geräte durch Eingabe einer PIN übernehmen darf oder nicht.

Darüber hinaus können Sie sehen, welchen Geräten dieser Benutzer als Hauptbenutzer zugeordnet ist, und ob der Benutzer gerade auf weiteren Geräten aktiv ist.

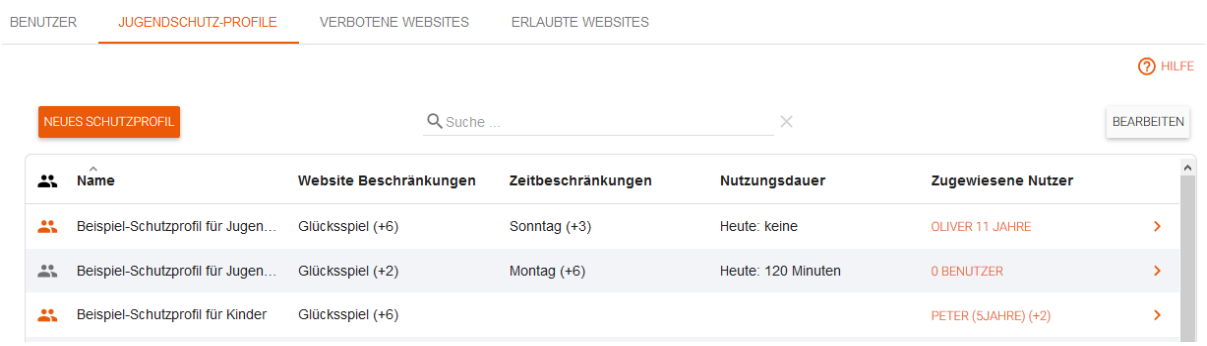
8.2.6 Benutzer entfernen

Über den Button „Benutzer entfernen“ in der Detailansicht zu einem Benutzer (s.o.) können Sie einen Benutzer auch wieder entfernen. Die Schaltfläche ist jedoch deaktiviert, wenn dem Benutzer noch Geräte zugeordnet sind. Weisen Sie den entsprechenden Geräten zunächst einen anderen Benutzer zu, um den Button zu aktivieren.

8.2.7 Neues Profil anlegen

Navigieren Sie in das Menü „eBlocker Einstellungen > Jugendschutz" und wählen Sie dort die Seite „Jugendschutz-Profile“:

Der eBlocker stellt ein Standard-Profil sowie ein paar Beispiel-Profile mit Jugendschutz-Einstellungen bereit:



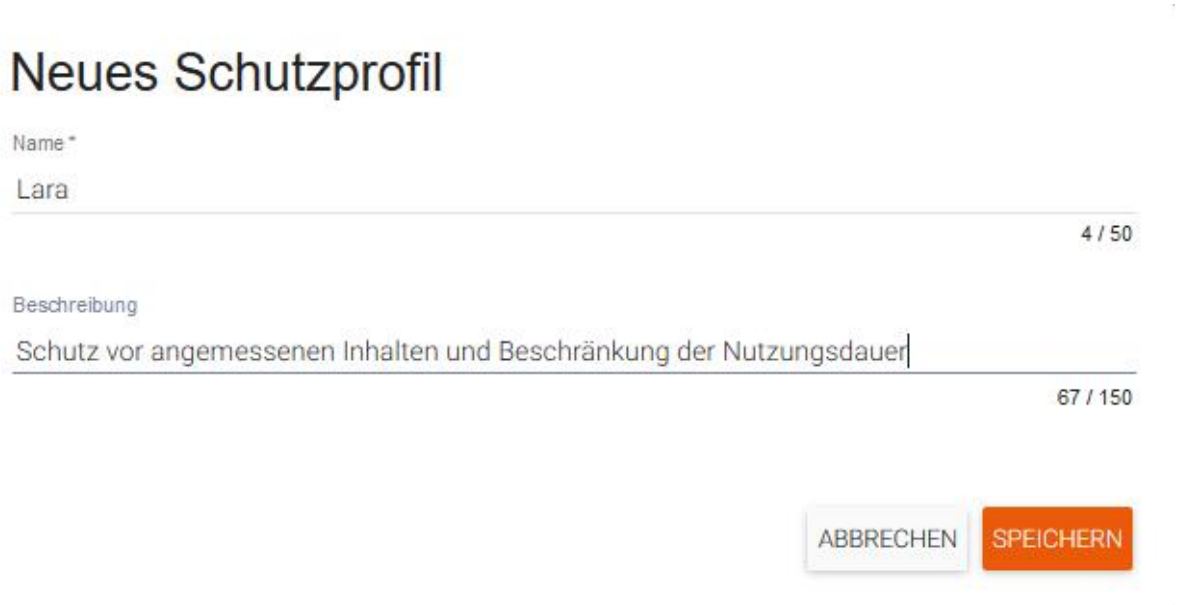
Das Standard-Profil sieht keine Beschränkungen des Internet-Zugangs vor. Es wird automatisch allen bestehenden und neuen Geräten im Heimnetz zugewiesen.

Darüberhinaus stellt der eBlocker vordefinierte Jugendschutz-Profile für unterschiedliche Anforderungen als Beispiel und Anregung bereit.

Klicken Sie auf den Button „Neues Schutzprofil", um ein neues Jugendschutz-Profil anzulegen.

Um Ihre Profile auseinander halten zu können, vergeben Sie entsprechende Namen und eine kurze Beschreibung.

Speichern Sie das Profil anschließend.

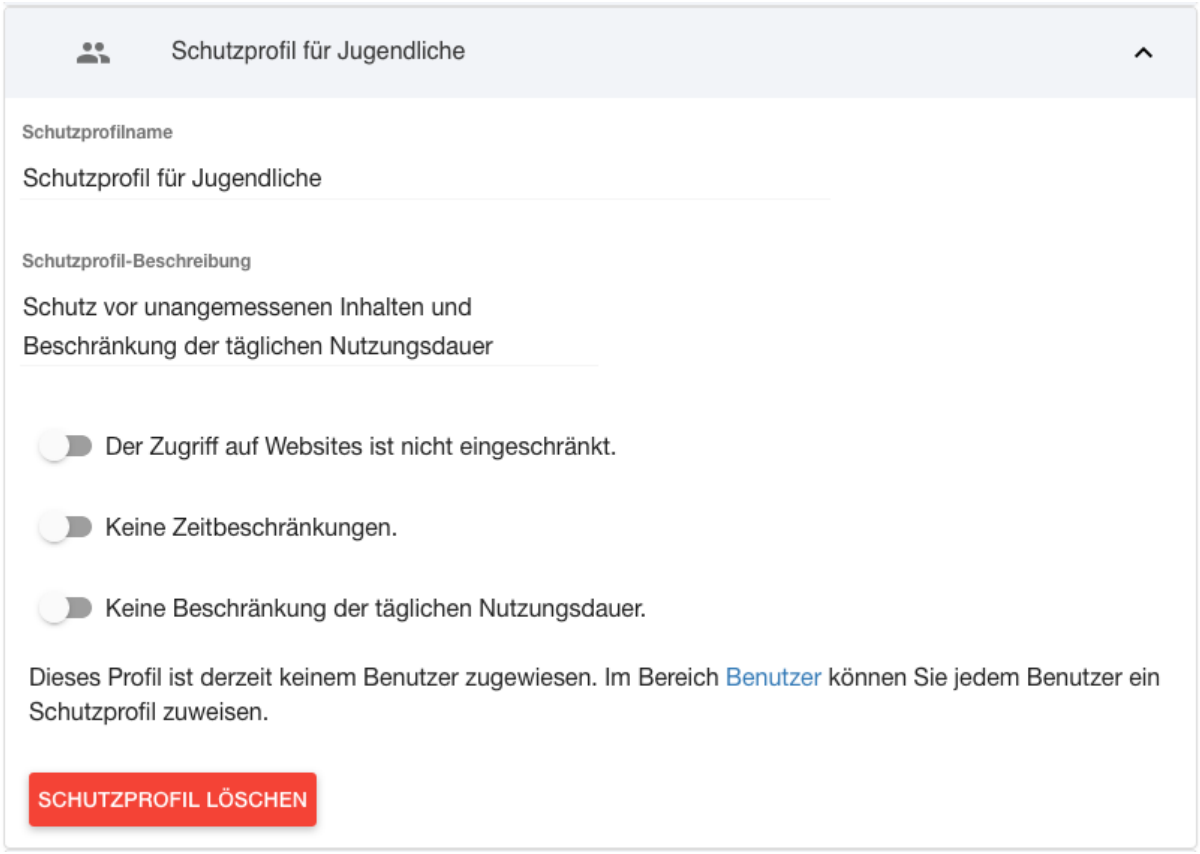


Um Zugriff auf die Einstellungen des soeben angelegten Profils zu erhalten, klicken Sie dieses in der Liste an.

Hier können Sie den Namen sowie die Beschreibung des Profils nachträglich ändern, die Website- und Kategorien-Filter bearbeiten, die Zeitbeschränkungen erstellen oder das Profil löschen.

In den Einstellungen des Profils sehen Sie auch, welchen Benutzern das Profil zur Zeit zugewiesen ist.

Zunächst sind in dem neuen Profil noch keine Jugendschutz-Beschränkungen aktiviert und dem Profil ist kein Benutzer zugewiesen:



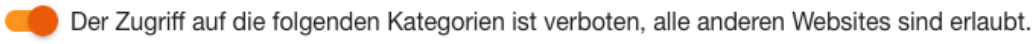
Sie können nun die folgenden Einstellungen vornehmen, um ein Jugendschutz-Profil nach Ihren Anforderungen zusammenzustellen:

- Den Zugriff auf bestimmt Kategorien von Websites verbieten oder erlauben.
- Den Internet-Zugriff nur zu bestimmten Tageszeiten erlauben.
- Die maximale Internet-Nutzungsdauer pro Tag beschränken.

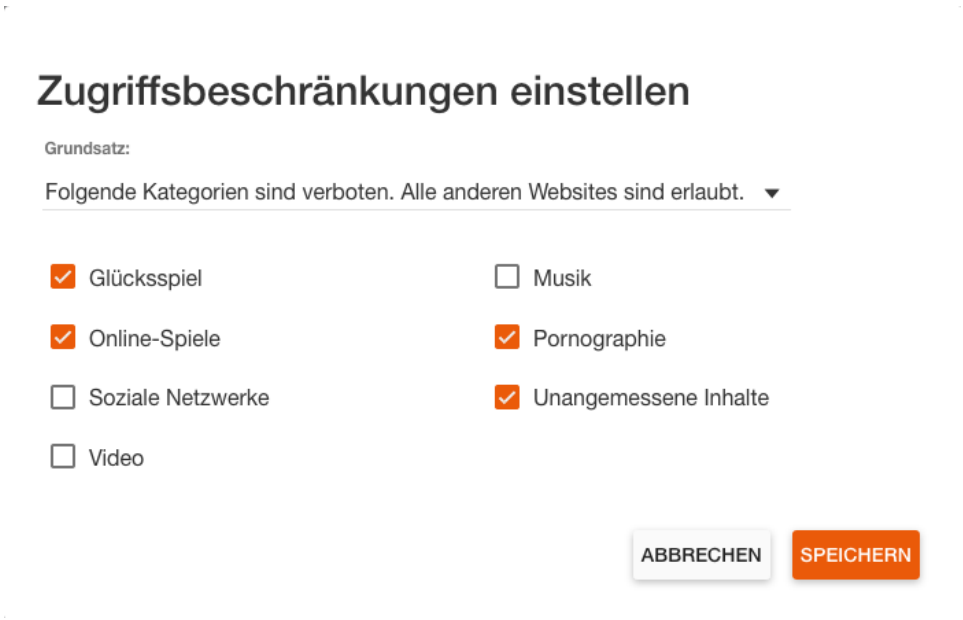
Details zu allen Einstellungsmöglichkeiten finden Sie in den nächsten Abschnitten.

8.2.8 Zugriff auf Kategorien von Websites verbieten

Um Zugriff auf bestimmte Kategorien von Websites zu verbieten, aktivieren Sie den Website-Kategorienfilter mit einem Klick auf den Schiebeschalter.

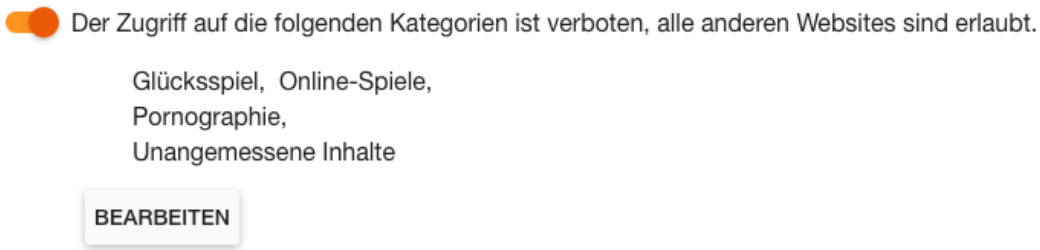


Es öffnet sich das folgende Dialogfenster:



Wenn Sie mit der Maus über die Liste der Kategorien fahren, werden Sie durch einen Tooltip über den Inhalt der Kategorien informiert. Wählen Sie hier die Kategorien aus, die für das Profil verboten werden sollen, und speichern Sie die Einstellungen.

Anschließend werden die Filter für dieses Profil generiert. Dies kann einige Sekunden dauern, da die Listen teilweise mehrere Millionen Einträge haben. Die Website-Kategorienfilter können Sie mit einem Klick auf den Button „Bearbeiten“ jederzeit anpassen:



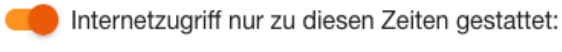
Weitere Details zu den Kategorien-Filtern und wie Sie selbst eigene Kategorien von verbotenen oder erlaubten Websites anlegen können, finden Sie in den Abschnitten 8.2.15 und 8.2.17.

Die von eBlocker bereitgestellten Kategorien-Filter werden täglich automatisch aktualisiert.

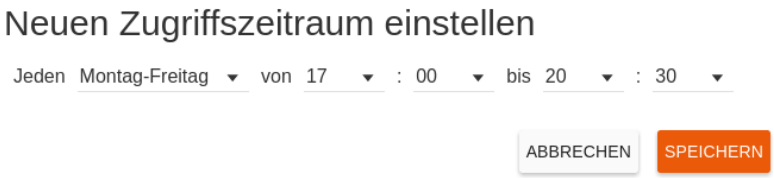
Um die Beschränkungen durch die Kategorien-Filter komplett abzuschalten, deaktivieren Sie den entsprechenden Schiebeschalter.

8.2.9 Internet-Zugriff nur zu bestimmten Tageszeiten erlauben

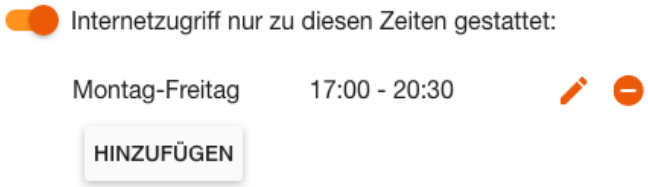
Sie können für jeden Wochentag einen oder mehrere Zeiträume festlegen, in denen der Internetzugriff durch dieses Profil gestattet ist. Aktivieren Sie dazu den Schiebschalter für die Zeitbeschränkung:



Wenn bisher noch keine Zeiträume festgelegt worden sind, öffnet sich direkt das folgende Dialogfenster:



Anschließend stellt sich die Konfiguration etwa so dar:



Um weitere Zeiträume hinzuzufügen, klicken Sie auf den Button „Hinzufügen“.

Um bereits festgelegte Zeiträume zu ändern, klicken Sie auf das Stiftsymbol neben dem Zeitraum.

Um Zeiträume wieder zu entfernen, klicken Sie auf das Minus-Symbol neben dem Zeitraum.

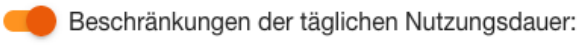
Um die Beschränkung auf Zeiträume komplett abzuschalten, deaktivieren Sie den entsprechenden Schiebeschalter.

8.2.10 Maximale Internet-Nutzungsdauer pro Tag beschränken

Zusätzlich zu den Zeiträumen, in denen Internet-Nutzung grundsätzlich gestattet ist, können Sie für jeden Wochentag eine maximale Internet-Nutzungsdauer festlegen.

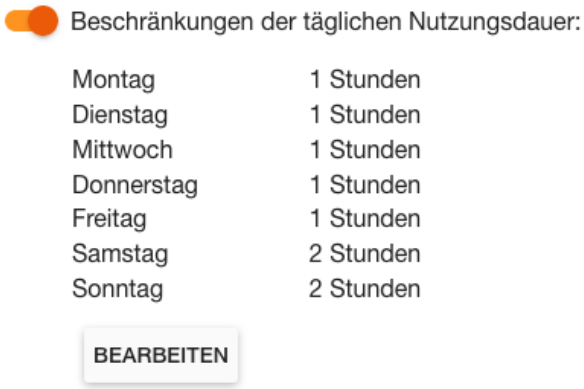
Es ist also z.B. möglich, die Internet-Nutzung grundsätzlich in der Zeit von 7h bis 20h zu gestattet, innerhalb dieses Zeitraums aber auf maximal eine Stunde zu beschränken.

Aktivieren Sie dazu den Schiebeschalter für die Beschänkung der maximalen täglichen Nutzungszeit:



Bei einem neu angelegten Jugendschutz-Profil ist die tägliche Nutzungsdauer auf 1 Stunde eingestellt. Klicken Sie auf den Button „Bearbeiten“, um die täglichen Nutzungsdauern zu verändern. Es öffnet sich der folgende Dialog:

Legen Sie für jeden Wochentag die maximale Nutzungsdauer fest und speichern Sie die Einstellungen. Anschließend stellt sich die Konfiguration etwa so dar:



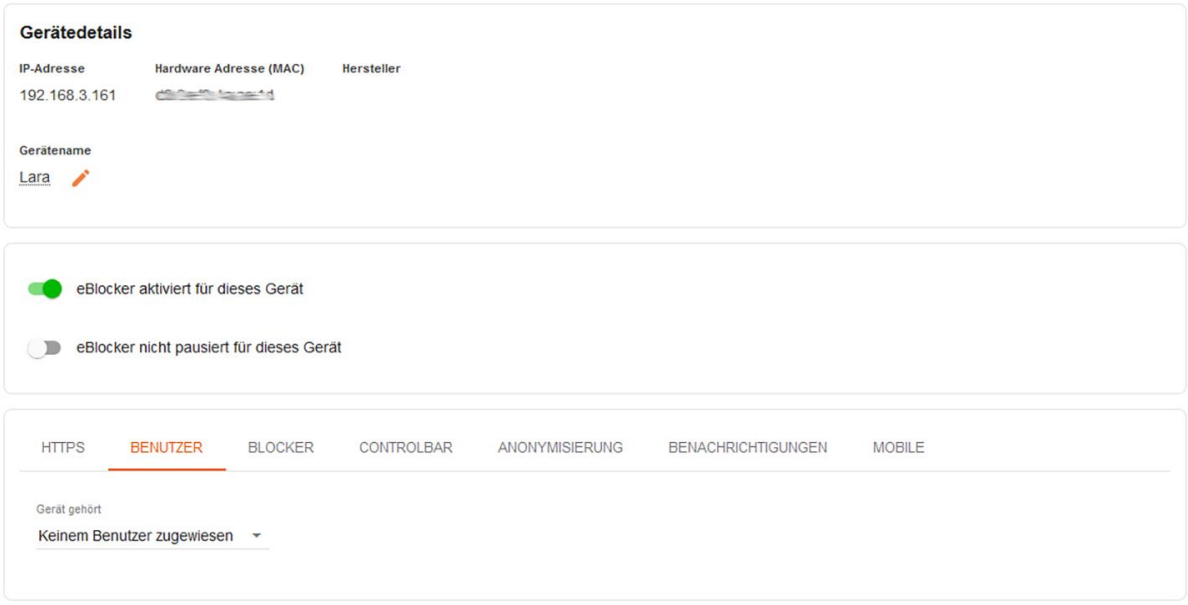
Um die Beschränkung auf maximale Nutzungsdauern komplett abzuschalten, deaktivieren Sie den entsprechenden Schiebeschalter.

Hinweis:
Jedem Benutzer, dem ein Profil mit einem Zeitkontingent zugeordnet wird, steht die entsprechende Online-Zeit komplett zur Verfügung und wird nicht unter verschiedenen Benutzern aufgeteilt.

8.2.11 Benutzer einem Gerät zuweisen

Um die Jugendschutz-Funktionen für ein Gerät zu aktivieren, muss diesem Gerät ein Benutzer als Hauptnutzer zugewiesen werden.

Navigieren Sie dazu bitte zu den „eBlocker Einstellungen > Geräte" (s. Abschnitt 8.3) und klicken Sie auf das Gerät, dem Sie einen Benutzer zuweisen wollen:

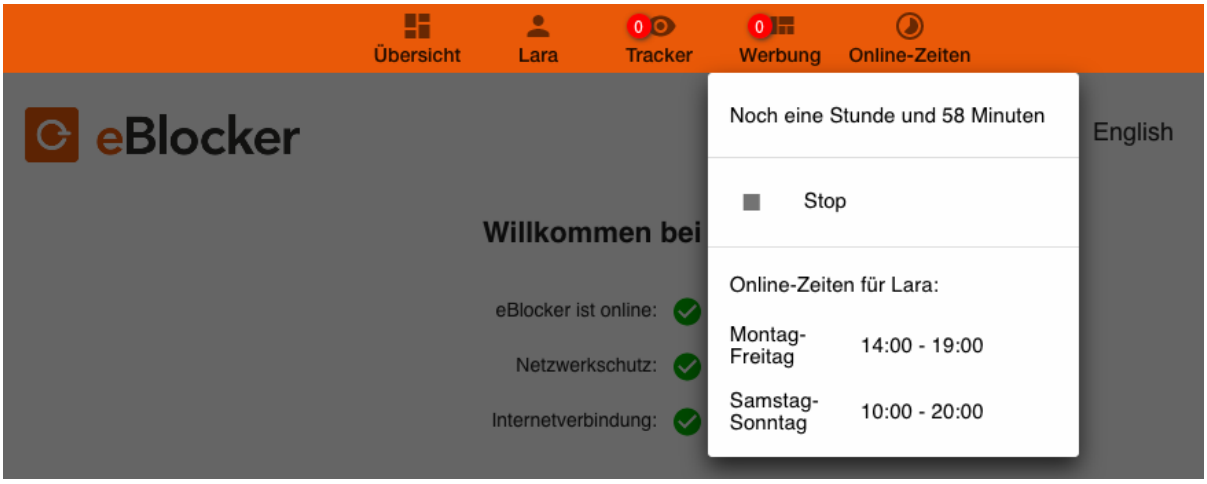


Zunächst ist ein neues Gerät keinem Benutzer zugewiesen. Klicken Sie auf die entsprechende Auswahlliste und wählen Sie den gewünschten Benutzer aus. Das Gerät unterliegt damit umgehend den Beschränkungen des Jugendschutz-Profils, das für den entsprechenden Benutzer eingestellt wurde.

Es ist möglich mehrere Geräte einem Nutzer zuzuweisen. Dann gelten auf allen seinen Geräten die selben Filterregeln und ein eingestelltes Zeitkontingent wird mit jedem seiner Geräte entsprechend der Nutzung verringert.

8.2.12 Controlbar für Benutzer mit Jugendschutz-Profilen

Wenn für einen Benutzer ein Jugendschutz-Profil eingestellt ist, dass eine oder mehrere Beschränkungen enthält, wird diesem Benutzer eine veränderte und eingeschränkte Controlbar zur Verfügung gestellt. Über den zusätzlichen Menüpunkt „Online-Zeiten“ können die aktuell verbleibende Internet-Nutzungsdauer, sowie die erlaubten Nutzungszeiten eingesehen werden:



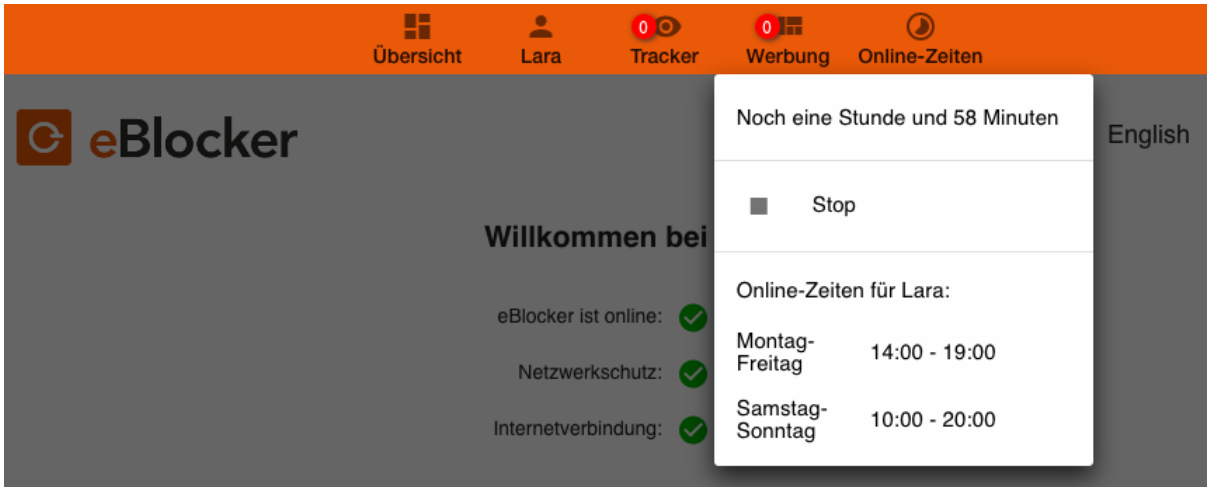
8.2.13 Was passiert, wenn die tägliche Internet-Nutzungsdauer beschränkt ist?

Wenn die tägliche Internet-Nutzungsdauer beschränkt ist, muss der Internet-Zugang explizit aktiviert werden. Anderenfalls würden automatische Prozesse des Betriebssystems oder von anderen Apps auf den Geräten die Nutzungszeit ungewollt „verbrauchen“, weil sie z.B. regelmäßig nach Updates suchen.

Daher wird zunächst die folgende Seite angezeigt, wenn der Benutzer versucht mit einem Internet-Browser auf eine beliebige Seite zu gehen:

Um die Internet-Nutzung zu aktivieren, muss der Schiebeschalter betätigt werden. Ab diesem Moment wird die verbleibende Nutzungszeit entsprechend reduziert. Die aktuell verbleibende Zeit wird jeweils angezeigt, um dem Benutzer eine flexible Zeiteinteilung zu ermöglichen.

Die aktuell verbleibende Nutzungsdauer kann auch jederzeit über das eBlocker-Icon und die Controlbar eingesehen werden. Auch hier besteht die Möglichkeit, die Internet-Nutzung zu beenden, um das Zeitkonto zu schonen:



Außerdem wird der Internet-Zugang automatisch nach einigen Minuten deaktiviert, wenn keine Internet-Nutzung stattfindet. Das dient ebenfalls dazu, das Zeitkonto nicht unnötig zu belasten.

8.2.14 Was passiert, wenn der Internet-Zugriff verweigert wird?

Bei Verwendung eines Internet-Browsers wird – je nach Grund für die Sperrung des Internet-Zugangs – eine der folgenden Meldungen angezeigt, um dem Nutzer transparent zu machen, dass und warum der Internet-Zugang verweigert wurde.

Bitte beachten Sie, dass andere Anwendungen und Apps bei blockiertem Internet-Zugang ggf. nicht mehr wie gewohnt funktionieren und unspezifische Fehlermeldungen ausgeben können. Die Anzeige einer entsprechenden Meldung durch den eBlocker ist bei solchen Anwendungen in der Regel nicht möglich.

Beschränkung durch Kategorien-Filter:

Wenn der Zugriff auf eine Website auf Grund eines Website-Kategorien-Filters unterbunden worden ist, bekommt der Benutzer anstelle der gewünschten Website die folgende Meldung des eBlocker zu sehen:

Über den Button „Konfiguration“ kann direkt die Einstellung der Jugendschutz-Funktion aufgerufen werden. Hierfür ist natürlich das Administrationspasswort erforderlich (s. Abschnitt 8.1.3).

Über den Button „Benutzer wechseln“ kann der aktive Benutzer des Geräts gewechselt werden. Wenn dieser Benutzer einem anderen Jugendschutz-Profil unterliegt, kann der Zugriff auf die fragliche Seite ggf. gestattet sein. Für den Wechsel zu einem anderen Benutzer muss jedoch die entsprechende Benutzer-PIN eingegeben werden.

Beschränkung bei Zugriff außerhalb eines erlaubten Zeitraums:

Wenn der Zugriff auf eine Webseite außerhalb eines erlaubten Zeitraums stattfindet, bekommt der Benutzer anstelle der gewünschten Website die folgende Meldung des eBlockers zu sehen:

Die Buttons „Konfiguration“ und „Benutzer wechseln“ haben die gleiche Funktion, wie oben beschrieben.

Wenn die maximale Nutzungsdauer pro Tag erreicht ist:

Wenn eine maximale Nutzungsdauer pro Tag festgelegt und bereits erreicht ist, wird die folgende Meldung angezeigt:

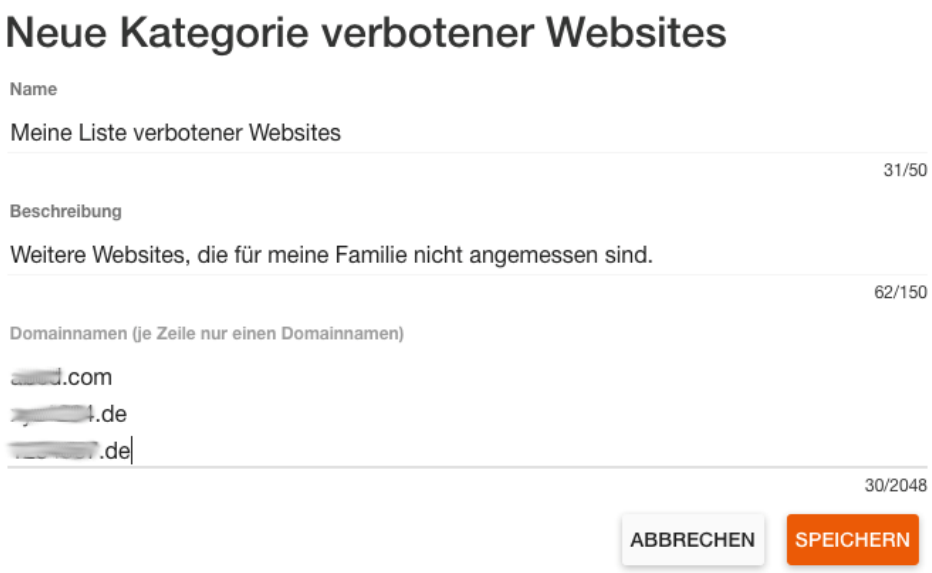
Die Buttons „Konfiguration“ und „Benutzer wechseln“ haben die gleiche Funktion, wie oben beschrieben.

8.2.15 Eigene Listen verbotener Websites anlegen

Navigieren Sie in das Menü „eBlocker Einstellungen > Jugendschutz" und wählen Sie dort die Seite „Verbotene Websites“:

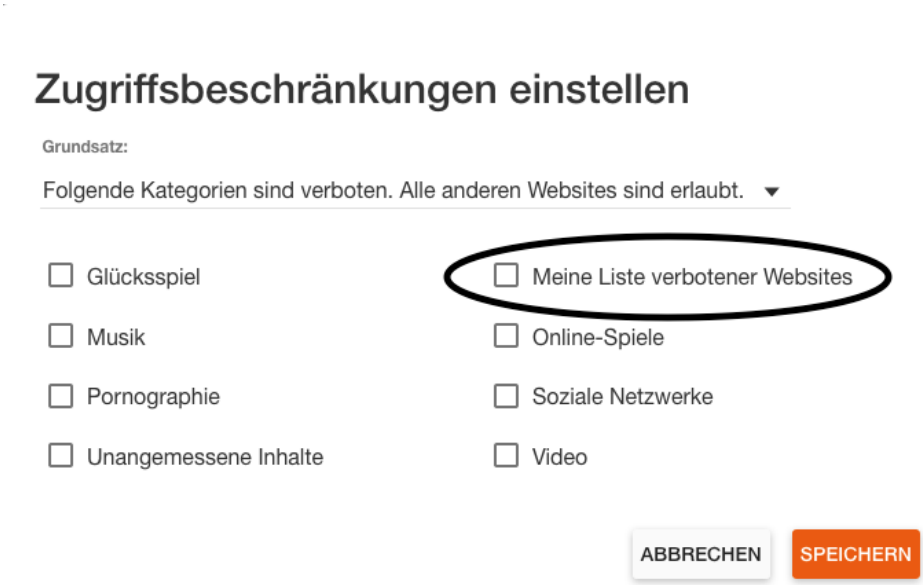
Der eBlocker stellt bereits eine Reihe von Listen verbotener Websites zu unterschiedlichen Kategorien bereit:

Sie können jederzeit selbst weitere Listen von Websites anlegen und in den Jugendschutz-Profilen verwenden. Klicken Sie dazu auf den Button „Neue Kategorie“. Es öffnet sich der folgende Dialog:



Sie können die eigenen Filter-Kategorien jederzeit einsehen, ergänzen oder wieder entfernen.

Alle eigenen Kategorien können genau wie die mitgelieferten Kategorien in den Jugendschutz-Profilen ausgewählt werden (s.a. Abschnitt 8.2.8):



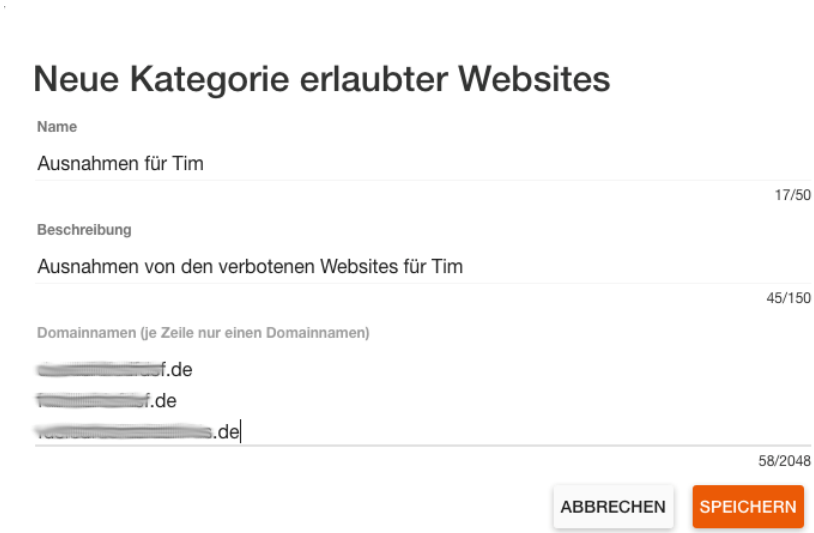
8.2.16 Ausnahmen zu den Kategorien verbotener Websites anlegen

Die mitgelieferten Kategorien verbotener Websites sind sehr umfassend und werden regelmäßig ergänzt und aktualisiert. Es kann natürlich vorkommen, dass die Listen in einzelnen Fällen zu streng sind und den Zugriff auf Websites verbieten, auf die Ihre Kinder Zugriff benötigen und auch erhalten sollen.

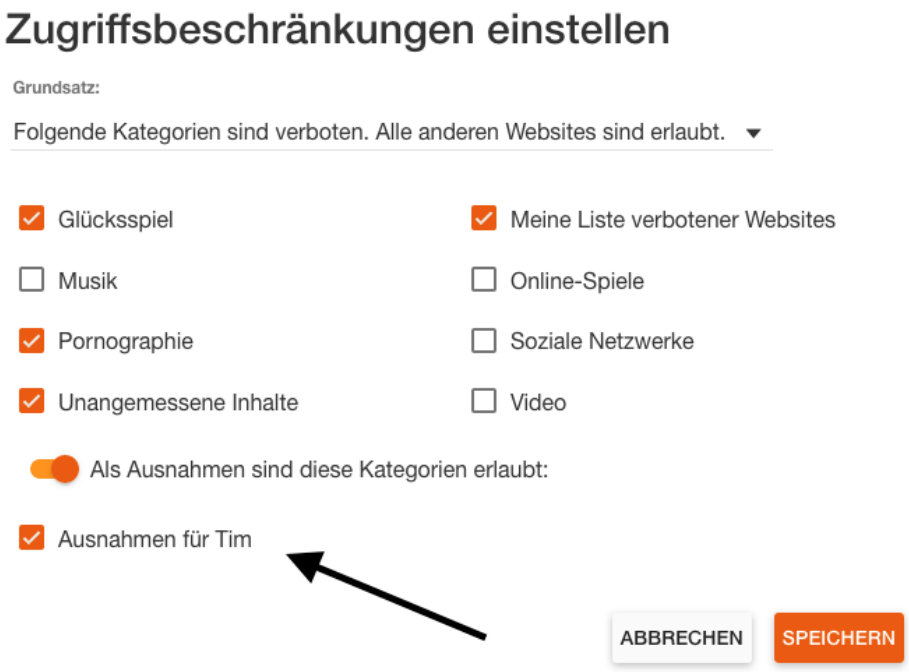
Damit Sie wegen einzelnen Websites nicht gleich die ganze Schutz-Kategorie abschalten müssen, können sie Ausnahmen definieren.

Navigieren Sie in das Menü „eBlocker Einstellungen > Jugendschutz" und wählen Sie dort die Seite „Erlaubte Websites“:

Legen Sie hier eine Kategorie mit Websites an, für die Sie den Zugriff ausdrücklich gestatten wollen. Zunächst ist die Liste der Kategorien mit erlaubten Websites leer. Klicken Sie auf den Button „Neue Kategorie“, um eine neue Kategorie anzulegen:



Sobald Sie eine oder mehrere Kategorien mit ausdrücklich erlaubten Websites angelegt haben, erscheinen diese als mögliche Ausnahmen bei der Konfiguration der Jugendschutz-Profile (s. Abschnitt 8.2.8):



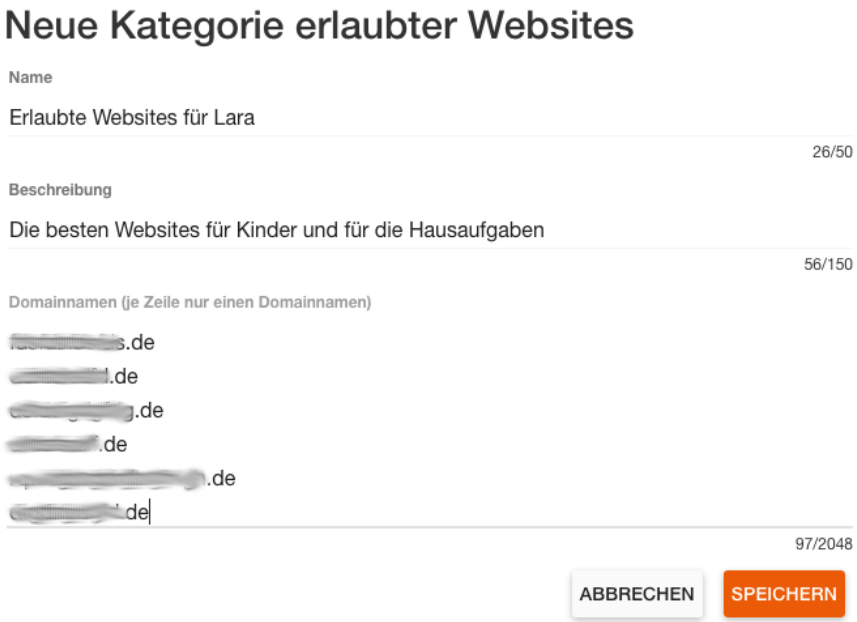
Aktivieren Sie den Schiebeschalter für die Ausnahmen, und wählen Sie die gewünschten Ausnahme-Kategorien aus.

8.2.17 Eigene Kategorien erlaubter Websites anlegen

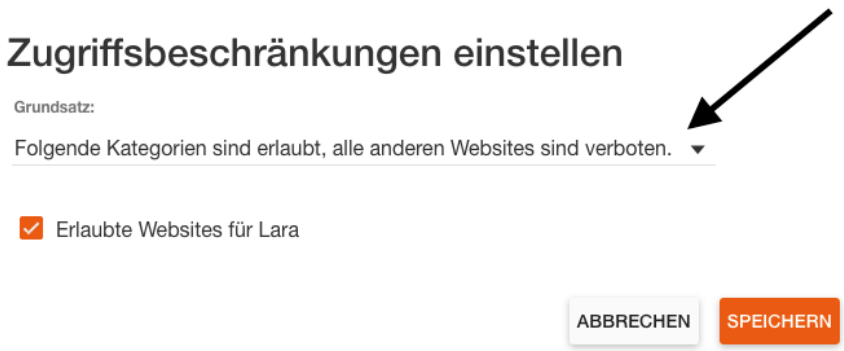
Anstatt den Internet-Zugriff durch Kategorien verbotener Websites zu beschränken, können Sie auch mit Kategorien ausdrücklich erlaubter Websites arbeiten. D.h. alles, was nicht ausdrücklich erlaubt ist, ist dann verboten.

Navigieren Sie auch dafür in das Menü „eBlocker Einstellungen > Jugendschutz" und wählen Sie dort die Seite „Erlaubte Websites“:

Legen Sie eine oder mehrere Kategorien von ausdrücklich erlaubten Websites an:



Auch diese Kategorien können Sie bei der Einrichtung eines Jugendschutz-Profils verwenden. Um mit ausdrücklich erlaubten Websites zu arbeiten, müssen Sie den Grundsatz bei der Zugriffsbeschränkung von „*alles was nicht ausdrücklich verboten ist, ist erlaubt*“ umstellen auf „*alles was nicht ausdrücklich erlaubt ist, ist verboten*“:

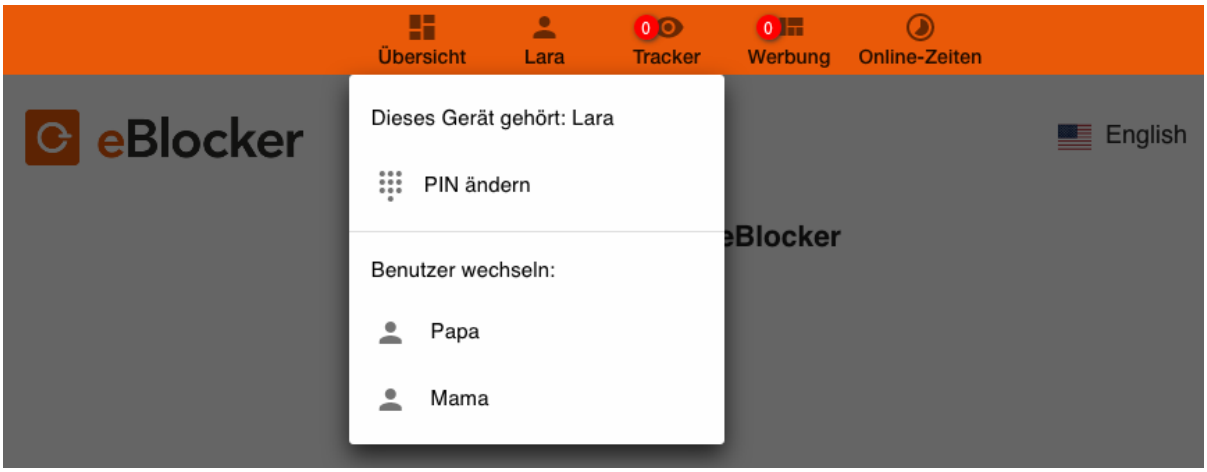


Beachten Sie, dass der Internet-Zugang durch solche Profile ganz erheblich eingeschränkt sein kann. So wird es ggf. auch nicht mehr möglich sein, Betriebssystem-Updates zu laden und viele Apps werden nicht wie gewohnt funktionieren.

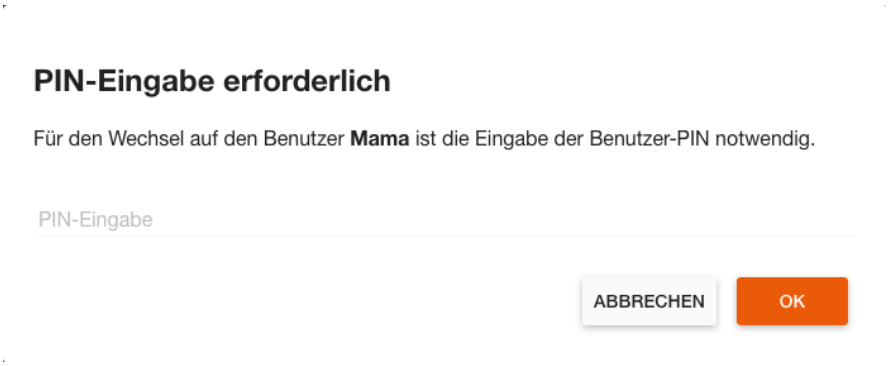
8.2.18 Wechsel des Benutzers über die Controlbar

Wenn für einen oder mehrere Benutzer eine PIN vergeben worden ist (s. Abschnitt 8.2.4), dann kann der aktuelle Benutzer eines Gerätes über die Controlbar geändert werden. Durch den Wechsel des Benutzers ändert sich ggf. auch das jeweils aktive Jugendschutz-Profil. So können die Zugriffsmöglichkeiten eines Gerätes recht flexibel und einfach geändert werden.

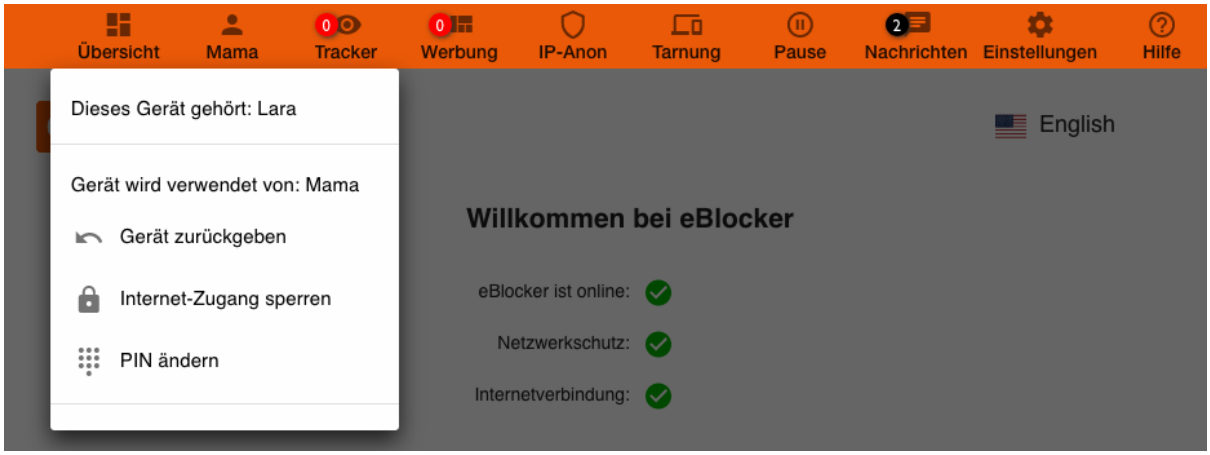
Angenommen, **Papa**, und **Mama** haben eine Benutzer-PIN, **Tim** und **Lara** jedoch nicht. Dann würde sich die Controlbar auf einem Gerät von Tim so darstellen:



Die Erwachsenen können also – durch Eingabe Ihrer PIN – das Gerät zeitweilig übernehmen und dadurch die Jugendschutz-Beschränkungen ebenfalls zeitweilig aufheben:



Nach der Übernahme des Gerätes stellt sich die Controlbar so dar:



In der Controlbar ist jederzeit sichtbar, wer der Hauptnutzer des Gerätes ist und wer das Gerät gerade verwendet. Außerdem gibt es die Möglichkeit, das Gerät an den Hauptnutzer zurückzugeben. Falls der Hauptnutzer selbst eine PIN gesetzt hat, ist auch für die Rückgabe die Eingabe der PIN nötig.

Einem Benutzer mit PIN stehen darüber hinaus zusätzliche Funktionen zur Verfügung:

- Sperren des Internet-Zugangs für das Gerät. Nur ein Benutzer mit PIN kann die Sperre aufheben.
- Ändern der eigenen PIN.

8.2.19 Migration der Jugendschutz-Funktion von eBlockerOS 1.0

Wenn Sie die Jugendschutz-Funktionen bereits unter eBlockerOS 1.0 verwendet haben, werden Sie bemerken, dass für jedes verwendete Jugendschutz-Profil ein Benutzer angelegt und den entsprechenden Geräten zugewiesen wurde.

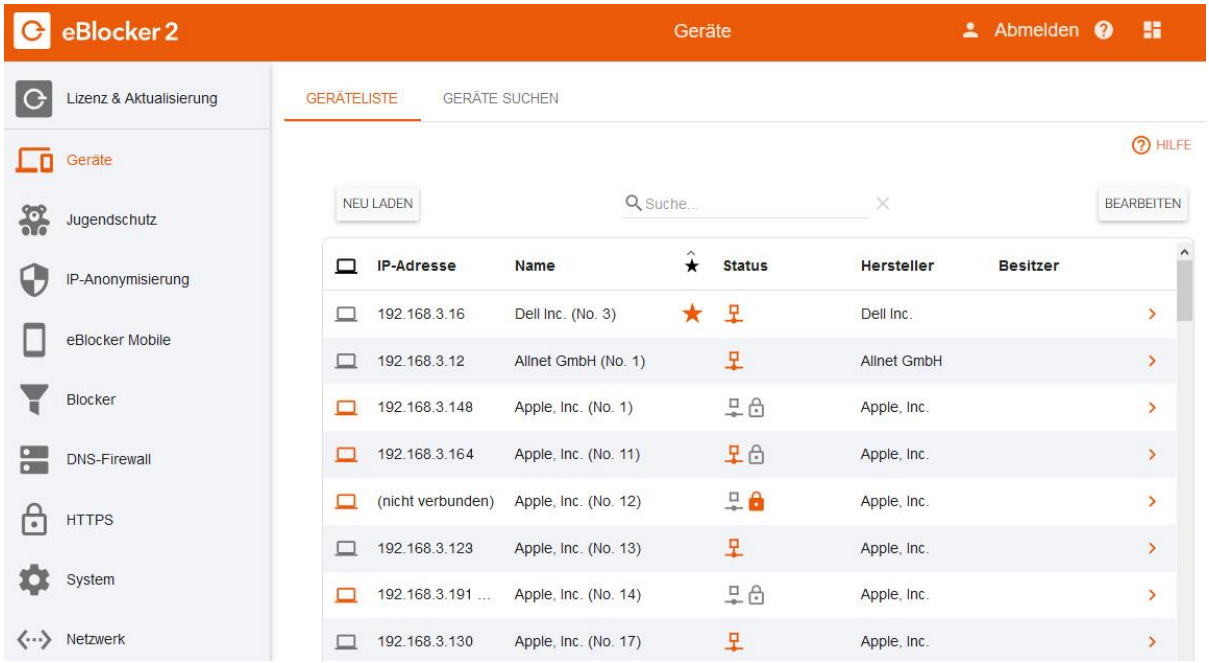
Das war notwendig, da die Profile nicht mehr direkt den Geräten zugeordnet sind.

An der Funktionsweise in Ihrem Heimnetz sollte sich durch diese Umstellung nichts geändert haben. Aber um alle Jugendschutz-Funktionen optimal nutzen zu können, sollten Sie die automatisch angelegten Benutzer umbenennen oder ersetzen und wenn nötig ergänzen.

8.3 Geräte

Gültig für **eBlocker Base**, **eBlocker Pro** und **eBlocker Family**

Die Funktion „Geräte“ zeigt Ihnen die Liste aller Netzwerkgeräte an, die der eBlocker in Ihrem Heimnetzwerk erkannt hat.



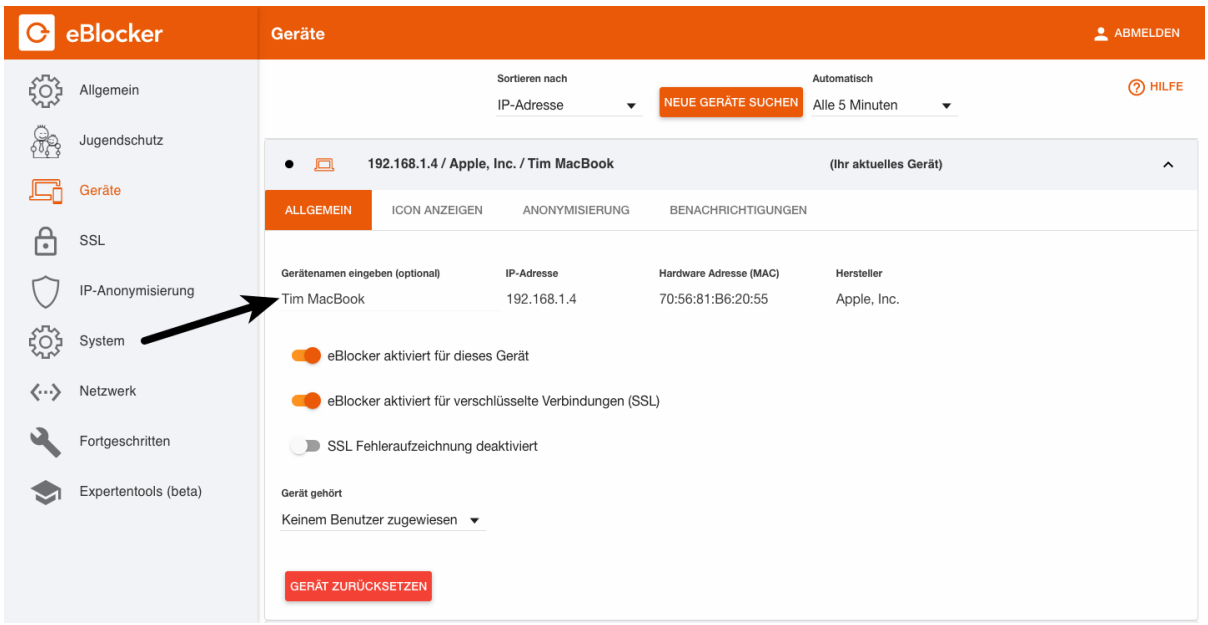
Die Geräte werden zunächst durch ihre IP-Adresse und – soweit der eBlocker das ermitteln kann – durch den Hersteller identifiziert. Durch einen Klick auf die IP-Adresse können Sie weitere Details zu dem Gerät öffnen und einige Einstellungen vornehmen.

Ihr Router und Ihr eBlocker haben ein eigenes graues Symbol. Bei beiden Geräten können Sie einen optionalen Namen vergeben, jedoch keine weiteren Einstellungen vornehmen.

Geräte mit einem orangem Symbol sind online, d.h. zur Zeit aktiv in Ihrem Netzwerk.

Geräte mit einem grauen Symbol waren online, d.h. zur Zeit nicht aktiv in Ihrem Netzwerk.

8.3.1 Geräte – Allgemein



8.3.2 Geräte – Allgemein - Namen

Wir empfehlen für alle Geräte einmalig einen Gerätenamen zu vergeben, damit Sie die Geräte jederzeit leicht wiedererkennen können (z.B.: „Christians Laptop“, „Fernseher Wohnzimmer“ oder „Sabines Smartphone“).

Hier werden Ihnen zusätzlich auch die IP Adresse, die Hardware Adresse (MAC) und gegebenenfalls der Hersteller pro Gerät angezeigt.

8.3.3 Geräte – Allgemein – eBlocker aktivieren

In der Grundeinstellung ist der eBlocker für die meisten Geräte automatisch aktiviert. Lediglich einige Gerätetypen (z.B. manche IP-Telefone und Hi-Fi-Komponenten) sind in der Grundeinstellung deaktiviert. Geräte, für die der eBlocker aktiviert ist, werden mit orangem Symbol dargestellt.

Sie können jederzeit für jedes Gerät individuell festlegen, ob es vom eBlocker überwacht werden soll oder nicht. Falls der eBlocker für das Gerät aktiviert wurde, stehen im Folgenden weiteren Funktionen zur Verfügung.

8.3.4 Geräte - HTTPS aktivieren

Kunden mit einem **eBlocker Pro** oder **eBlocker Family**, können hier, wenn die HTTPS-Funktionalität auf dem eBlocker grundsätzlich aktiviert ist (siehe Abschnitt 8.4.1), den eBlocker für jedes Gerät einzeln beauftragen, auch verschlüsselte Verbindungen (HTTPS) zu überwachen.

8.3.5 Geräte - Benutzer

eBlocker Family Kunden können hier bestimmen, ob das Gerät zu einem bestimmten Benutzer zugeordnet werden soll.

8.3.6 Geräte - Blocker

Hier bestimmen Sie, ob der eBlocker Tracker und Ads blockieren soll, ob der eBlocker seinen „Domain Blocker“, oder ob der eBlocker seinen „Pattern Blocker“ benutzen soll. Die Einstellung „Pattern Blocker“ setzt die Aktivierung von der HTTPS Funktion vor aus.

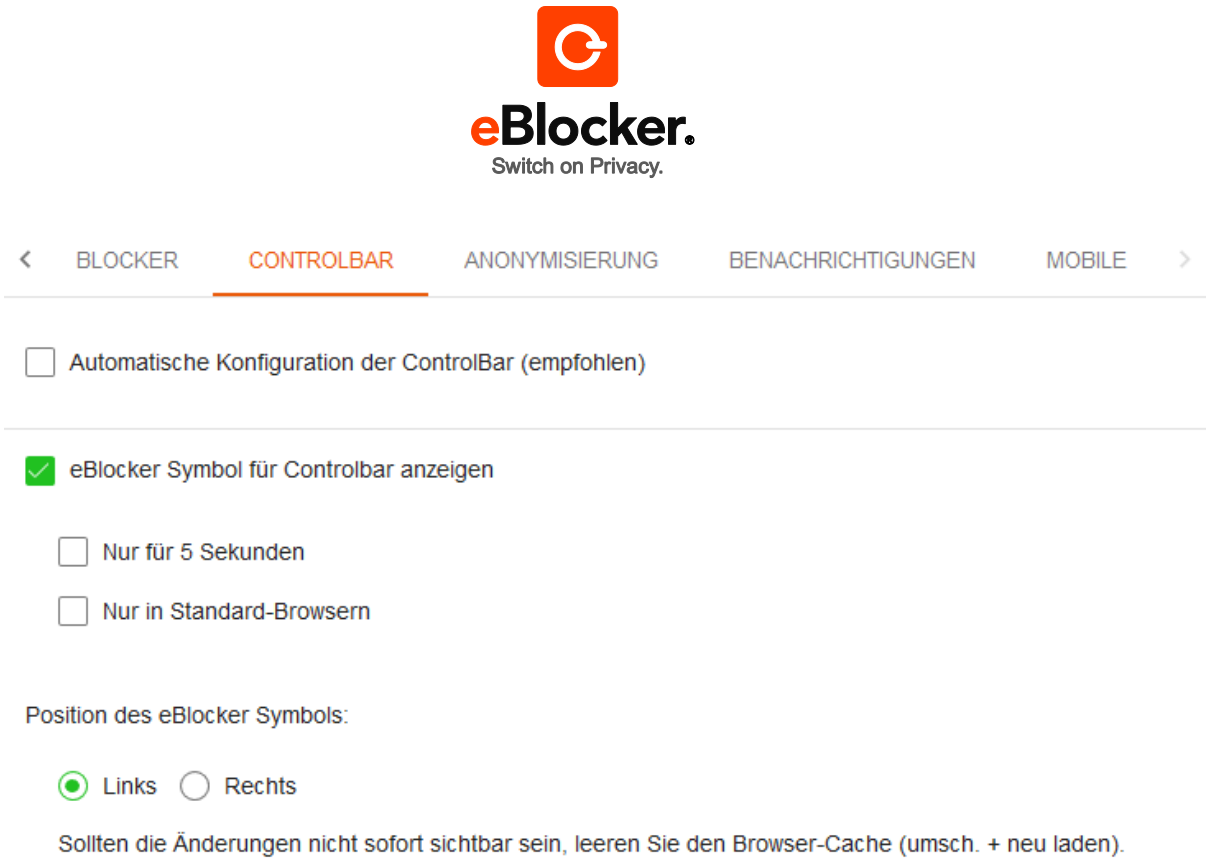
Wenn Sie die Einstellung auf Automatisch setzen, wird der eBlocker anhand der HTTPS Funktion (aktiviert oder deaktiviert) für Sie entscheiden, ob der Domain, oder Pattern Blocker benutzt wird. Wir empfehlen die Einstellung „Automatisch“ zu verwenden.

8.3.7 Geräte - Controlbar

Legen Sie hier fest, ob das eBlocker Symbol (siehe Abschnitt 7.1) auf dem Gerät immer, nie oder nur für fünf Sekunden angezeigt werden soll, sobald Sie eine neue Webseite aufrufen.

Zusätzlich gibt es die Option, das eBlocker Symbol nur in Standard-Browsern wie Microsoft Edge, Firefox, Chrome, oder Safari einzublenden. Dies umfasst auch Browser welche auf Chrome oder Firefox basieren. Das eBlocker Symbol wird dann beispielsweise nicht in Apps angezeigt.

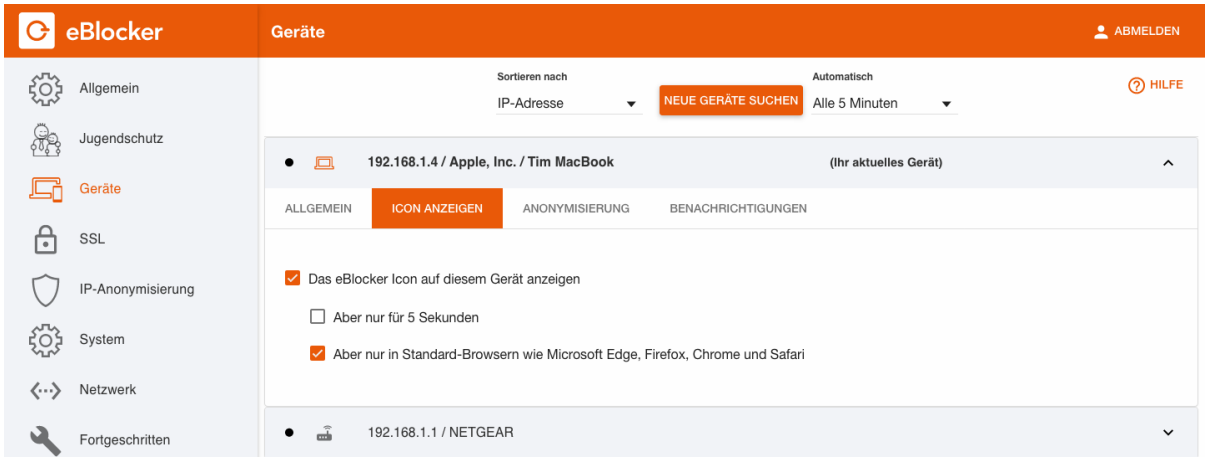
Außerdem können Sie hier die Position des eBlocker Symbols festlegen.



8.3.8 Geräte - Allgemein Icon anzeigen

Hier können Sie hier festlegen, ob das eBlocker Icon (siehe Abschnitt 7.1) auf dem Gerät immer, nie oder nur kurz für fünf Sekunden angezeigt werden soll, sobald Sie eine neue Webseite aufrufen.

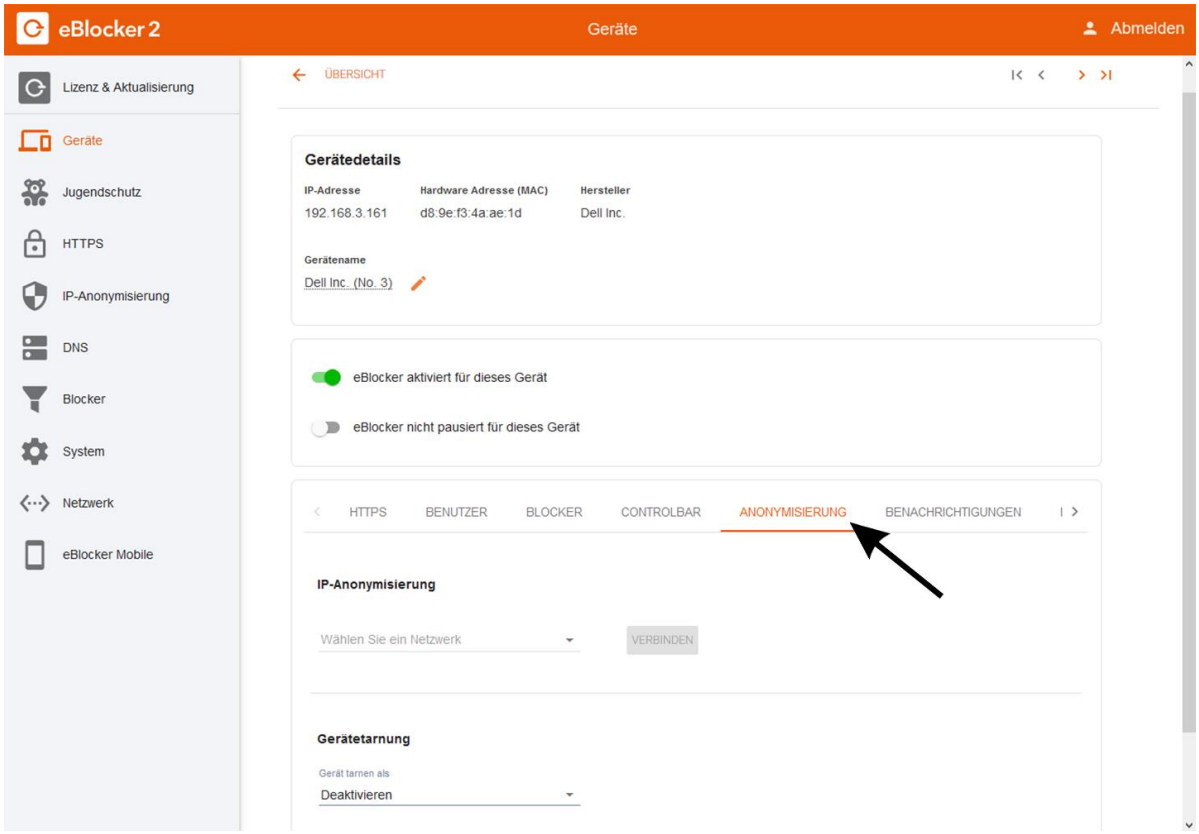
Zusätzlich gibt es die Option, das eBlocker Icon nur in Standard-Browsern wie Microsoft Edge, Firefox, Chrome, oder Safari einzublenden. Dies umfasst auch Browser, welche auf Chrome oder Firefox basieren. Das eBlocker Icon wird dann zum Beispiel nicht in Apps angezeigt.

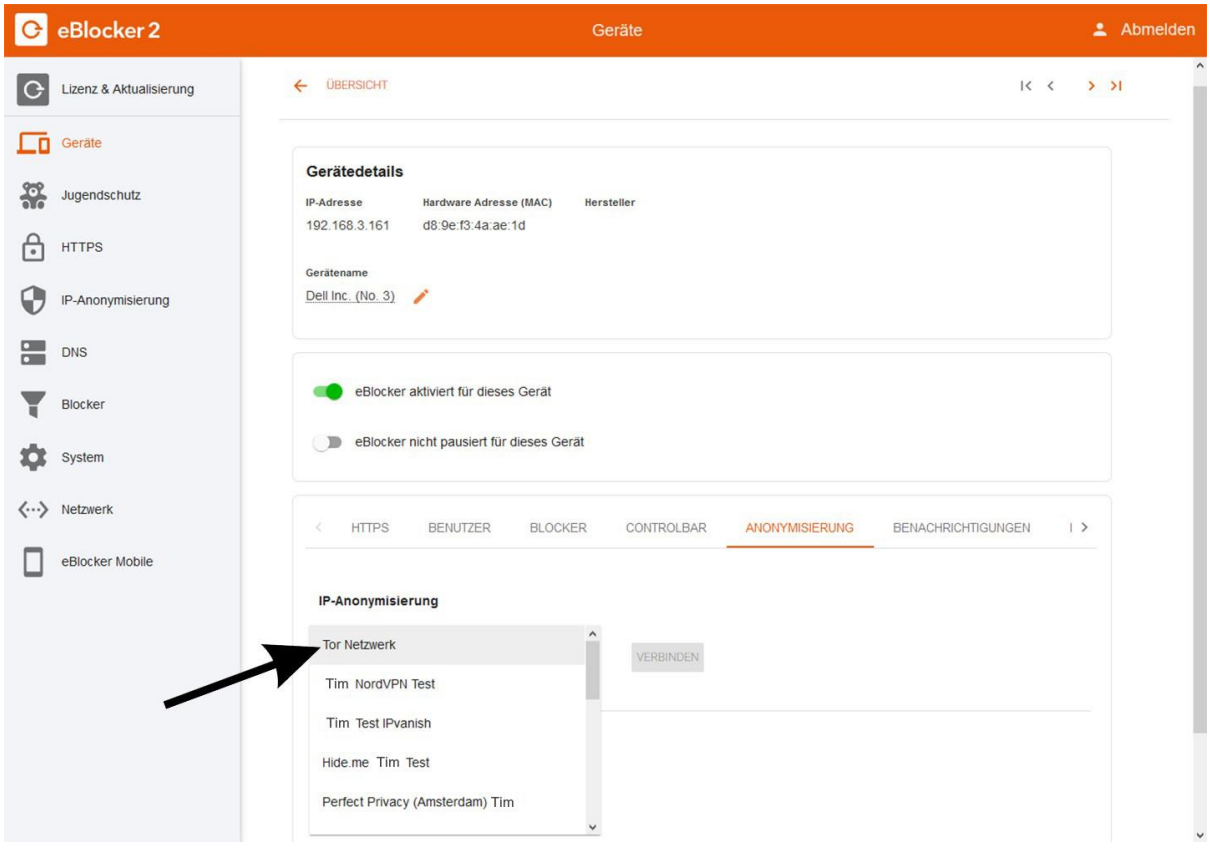


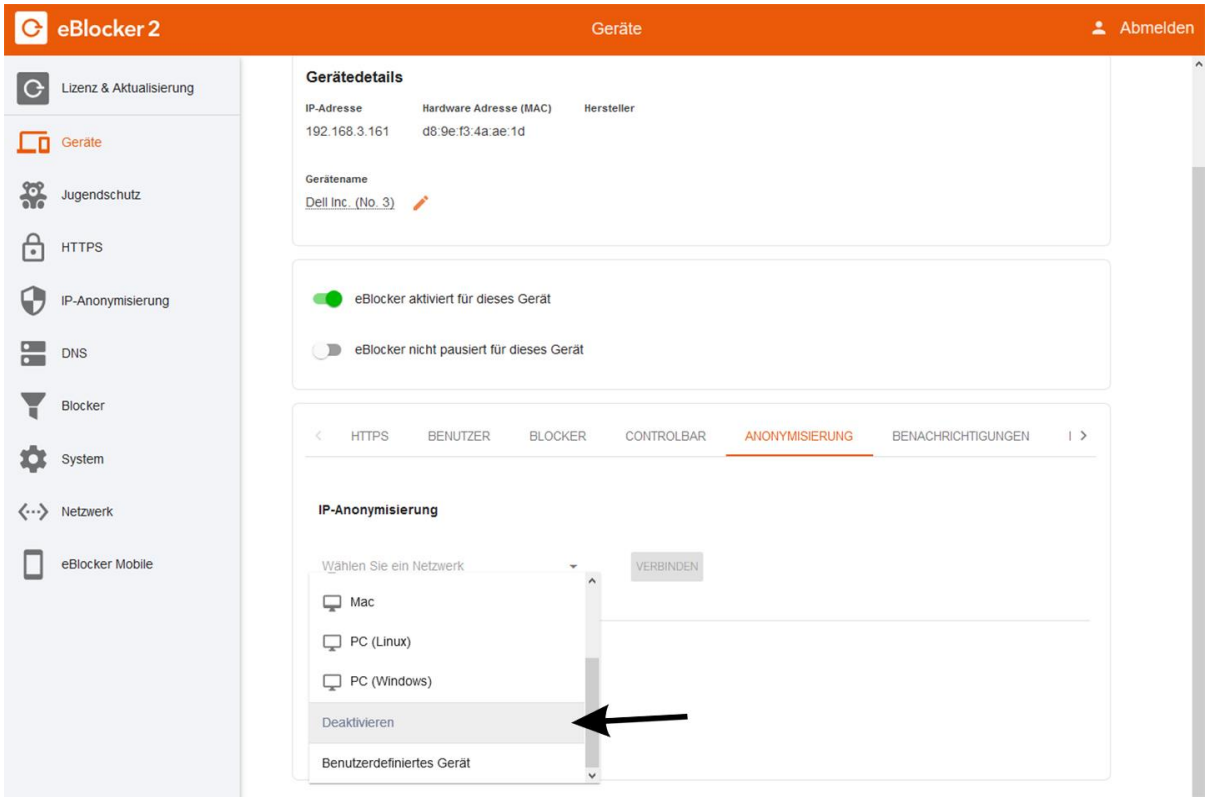
8.3.9 Geräte Anonymisieren

Aktivieren Sie die IP-Anonymisierung und bestimmen Sie ob eine Tor- oder VPN-Verbindung benutzen möchten.

Zusätzlich können Sie hier die Tarnung für ein Gerät bestimmen. Öffnen Sie dazu die Auswahl und wählen Sie einen der vordefinierten Tarnungen (User Agenten) aus oder geben Sie einen eigenen User Agenten ein (siehe dazu Abschnitt 7.6).

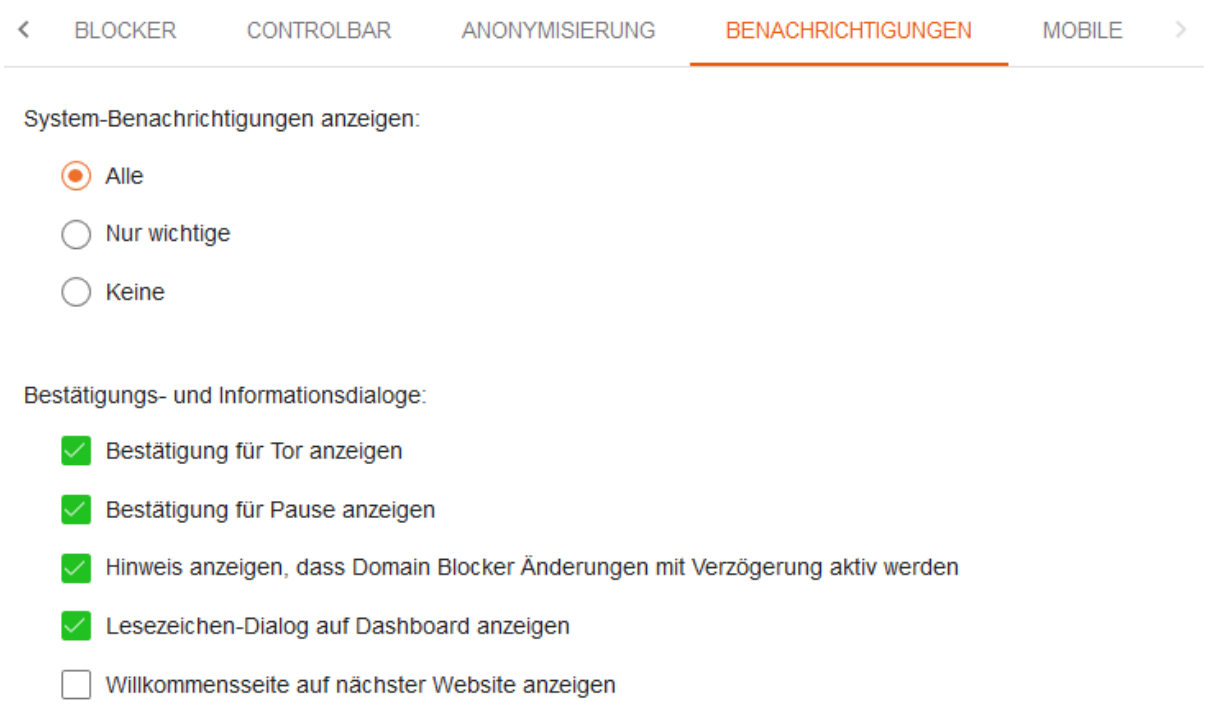

eBlocker 2
Geräte
Abmelden
Lizenz & Aktualisierung
Geräte
Jugendschutz
HTTPS
IP-Anonymisierung
DNS
Blocker
System
Netzwerk
eBlocker Mobile
ÜBERSICHT
Gerätedetails
IP-Adresse
192.168.3.161
Hardware Adresse (MAC)
d8:9e:f3:4a:ae:1d
Hersteller
Dell Inc.
Gerätename
Dell Inc. (No. 3)
eBlocker aktiviert für dieses Gerät
eBlocker nicht pausiert für dieses Gerät
HTTPS
BENUTZER
BLOCKER
CONTROLBAR
ANONYMISIERUNG
BENACHRICHTIGUNGEN
IP-Anonymisierung
Wählen Sie ein Netzwerk
VERBINDEN
Gerätetarnung
Gerät tarnen als
Deaktivieren


eBlocker 2
Geräte
Abmelden
Lizenz & Aktualisierung
Geräte
Jugendschutz
HTTPS
IP-Anonymisierung
DNS
Blocker
System
Netzwerk
eBlocker Mobile
ÜBERSICHT
Gerätedetails
IP-Adresse
192.168.3.161
Hardware Adresse (MAC)
d8:9e:f3:4a:ae:1d
Hersteller
Gerätename
Dell Inc. (No. 3)
eBlocker aktiviert für dieses Gerät
eBlocker nicht pausiert für dieses Gerät
HTTPS
BENUTZER
BLOCKER
CONTROLBAR
ANONYMISIERUNG
BENACHRICHTIGUNGEN
IP-Anonymisierung
Tor Netzwerk
Tim NordVPN Test
Tim Test IPvanish
Hide.me Tim Test
Perfect Privacy (Amsterdam) Tim
VERBINDEN



8.3.10 Geräte – Benachrichtigungen

Hier können Sie pro Gerät bestimmen, ob alle, die wichtigsten oder keine Systemnachrichten vom eBlocker angezeigt werden sollen.



Als Standard Einstellung für alle Geräte, werden alle Systemnachrichten vom eBlocker angezeigt.

8.3.11 Geräte - Mobile

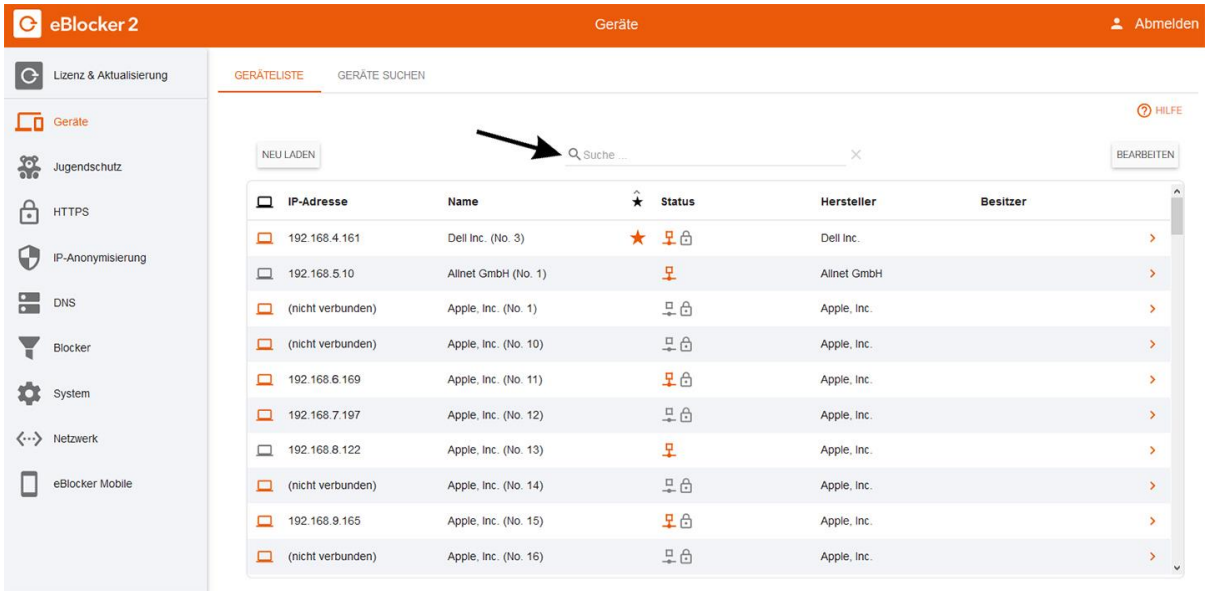
Hier können Sie - sofern die eBlocker Mobile Funktion aktiviert wurde - den Zugriff auf Ihren eBlocker für dieses Gerät von außerhalb Ihres Netzwerkes aktivieren.

Sie können bestimmen, ob dieses Gerät nur für den Internetzugriff aktiviert ist, oder ob man von dem Gerät auch von außerhalb Ihres Netzwerkes den eBlocker konfigurieren kann.

8.3.12 Geräte - Neue Geräte entdecken oder Gerät aus der Liste entfernen

Der eBlocker erkennt neue Geräte in Ihrem lokalen Netzwerk i.d.R. nach kurzer Zeit automatisch und zeigt sie auf der Seite „Geräte“ an. Mit einem Klick auf die Schaltfläche „Neue Geräte entdecken“, können Sie jederzeit manuell nach neuen Geräten suchen.

Sie können festlegen, ob der eBlocker nun alle 10 Sekunden, alle 5 Minuten, oder nie nach neuen Geräten suchen soll. Sollten Sie die Option "Nie" auswählen, dann beachten Sie bitte, dass Sie immer manuell nach neuen Geräten suchen müssen.



Geräte, die vom eBlocker nicht mehr gefunden werden, werden jedoch nicht automatisch entfernt. Der eBlocker kann nicht wissen, ob das Gerät nur kurzzeitig ausgeschaltet oder offline ist, oder ob es tatsächlich nicht mehr existiert. Unten auf der Seite haben Sie die Möglichkeit entweder alle Geräte ohne IP Adresse zu entfernen, alle Offline-Geräte zu entfernen oder alle Geräte zu entfernen. Wählen die ggf. eine dieser Optionen aus und klicken Sie auf die Schaltfläche "Auswahl entfernen".

8.4 HTTPS

Gültig für **eBlocker Pro** und **eBlocker Family**

SSL steht für Secure Sockets Layer und ist ein Protokoll, um die Kommunikation „Ende-zu-Ende“ zwischen zwei Kommunikationspartnern zu verschlüsseln. Manchmal wird Ihnen vielleicht auch die Abkürzung TLS begegnen (TLS steht für Transport Layer Security). Sie bezeichnet im Grunde das gleiche wie SSL. Wird das Standard-Webprotokoll HTTP mit Hilfe von SSL verschlüsselt, so wird es

als HTTPS bezeichnet. Sie erkennen eine verschlüsselt geladene Seite daran, dass die URL mit https:// beginnt. Viele Browser zeigen in der Adresszeile zusätzlich ein grünes Schloss an.

Viele Webseiten, insbesondere von Banken und Online-Shops sind heute mit SSL-Verschlüsselung geschützt. Dadurch können Sie sicher sein, dass Sie tatsächlich mit dem Anbieter kommunizieren dessen URL Sie aufgerufen haben und dass kein Dritter Ihre eingegebenen Daten verändern oder mitlesen kann. Allerdings verwenden nicht nur seriöse Shops und Banken SSL. Auch Tracking- und Werbeanbieter sammeln ihre Daten immer öfter über HTTPS/SSL. Ihre Profildaten werden dann zwar verschlüsselt zum Trackingserver geschickt, aber das hindert den Datensammler natürlich nicht daran, weiterhin ein detailliertes Profil von Ihnen zu erstellen.

Sobald die SSL-Unterstützung im eBlocker aktiviert wird, generiert jeder eBlocker ein eindeutiges Geräte-Stammzertifikat und einen privaten Schlüssel. Dieses Zertifikat wird genutzt, um die Kommunikation zwischen Ihrem Gerät und dem eBlocker zu verschlüsseln, wenn der eBlocker eine mit SSL geschützte Webseite lädt.

Sobald SSL aktiviert wurde, terminiert der eBlocker die verschlüsselte Verbindung, damit der Datenstrom analysiert werden kann. Der eBlocker ist damit das Ende der „Ende-zu-Ende Verschlüsselung“. Da der Browser bei HTTPS eine verschlüsselte Verbindung erwartet, verschlüsselt der eBlocker anschließend die Kommunikation zu Ihrem Endgerät. Dazu ist es notwendig einmalig das sogenannte Sicherheitszertifikat Ihres eBlockers erst in Ihrem Betriebssystem und dann gegebenenfalls in den Browsern mit einem eigenen Zertifikatsspeicher wie im Abschnitt 6.2 beschrieben aufzunehmen. Dieses Zertifikat wird manchmal auch als Zertifikat für Zertifizierungsstellen, als Stammzertifikat oder als Root-Zertifikat bezeichnet.

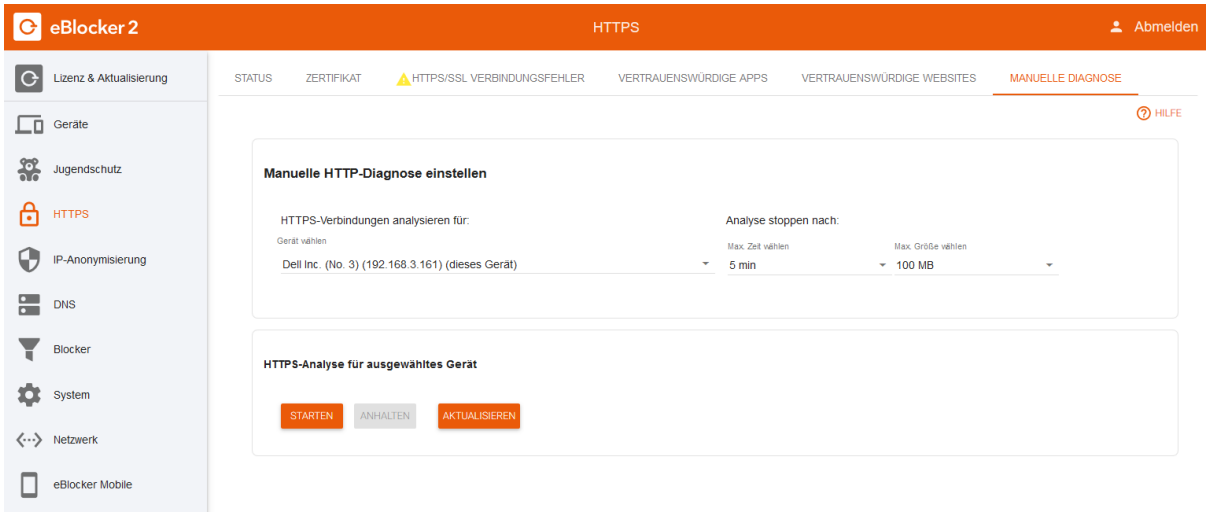
Wir haben weder Zugang zu Ihrem privaten Schlüssel noch zu Ihrem Gerät und haben alles dafür getan, um den eBlocker vor Hackern zu schützen – aber natürlich gibt es keine 100 prozentige Sicherheit. Wir bieten die SSL-Unterstüzung als Option an. Sollten Sie sich unwohl damit fühlen, dass der eBlocker die SSL-Verbindung entschlüsselt, aktivieren Sie diese Option bitte nicht.

Oder setzen Sie die Webseiten, denen Sie vertrauen, und in deren Veschlüsselung der eBlocker nicht hineinschauen soll, auf die Liste der vertrauenswürdigen Webseiten. Auf diese Seiten kann der eBlocker dann allerdings zum Beispiel keine Tracker erkennen und blockieren, und auch das eBlocker Icon kann nicht eingeblendet werden (s. auch Abschnitt 8.4.4).

8.4.1 HTTPS - Status

Um SSL zu aktivieren, klicken Sie auf das eBlocker Icon oben rechts in Ihrem Browserfenster und gehen Sie auf „Einstellungen“. Klicken Sie auf den Menüpunkt „SSL“.

Sie befinden sich nun in dem Reiter „Status“. Aktivieren Sie hier die SSL Funktion für Ihren eBlocker, indem Sie den Button nach rechts schieben.



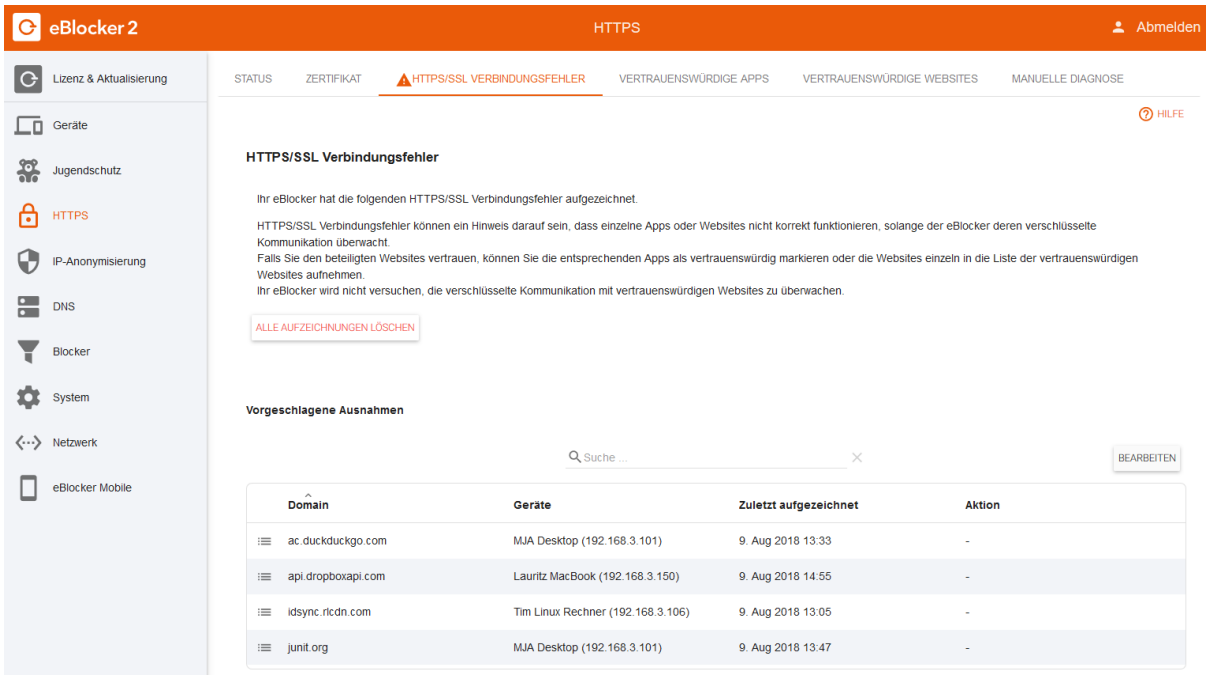
Bitte beachten Sie, dass das Zertifikat erst in Ihrem Betriebssystem und dann gegebenenfalls noch in Browsern mit eigenem Zertifikatsspeicher hinterlegt werden muss. Siehe Kapitel 6.2 „Die Aufnahme des eBlocker-Zertifikats“.

Klicken Sie auf „Hilfe - wie man das Zertifikat im Browser aufnimmt“, um eine ausführliche Erklärung für das Aufnehmen des Zertifikats zu erhalten.

Manche Apps oder Websites funktionieren nicht korrekt, wenn der eBlocker deren verschlüsselte Kommunikation überwacht. Wenn Sie die Funktion „Aufzeichnung von Verbindungsfehlern“ aktivieren, dann zeichnet der eBlocker die problematischen Verbindungen auf. Diese Aufzeichnungen können sehr hilfreich sein, um betroffene Apps und Websites zu identifizieren.

8.4.2 HTTPS – Verbindungsfehler

Wenn Sie die Funktion „Aufzeichnung von Verbindungsfehlern“ aktiviert haben, dann sehen Sie hier gegebenenfalls eine Liste der Verbindungsfehler.



Sie können die gefundenen Verbindungsfehler ganz bequem zu einer App Ausnahmeliste („vertrauenswürdige App“) hinzufügen, oder als „vertrauenswürdige Website“ festlegen, in dem Sie die gefundene Domain Auswählen und dann eine der drei folgenden Möglichkeiten auswählen.

Neue Vertrauenswürdige App

Hiermit legen Sie mit den ausgewählten Domains eine neue Ausnahmeliste an, welche Sie dann in dem Reiter „Vertrauenswürdige Apps“ wieder finden.

Zu App hinzufügen

Hiermit fügen Sie die Auswahl der Domains zu einer bestehenden App Ausnahmeliste aus dem Reiter „Vertrauenswürdige Ausnahmen“ hinzu.

Zur Ausnahmeliste hinzufügen

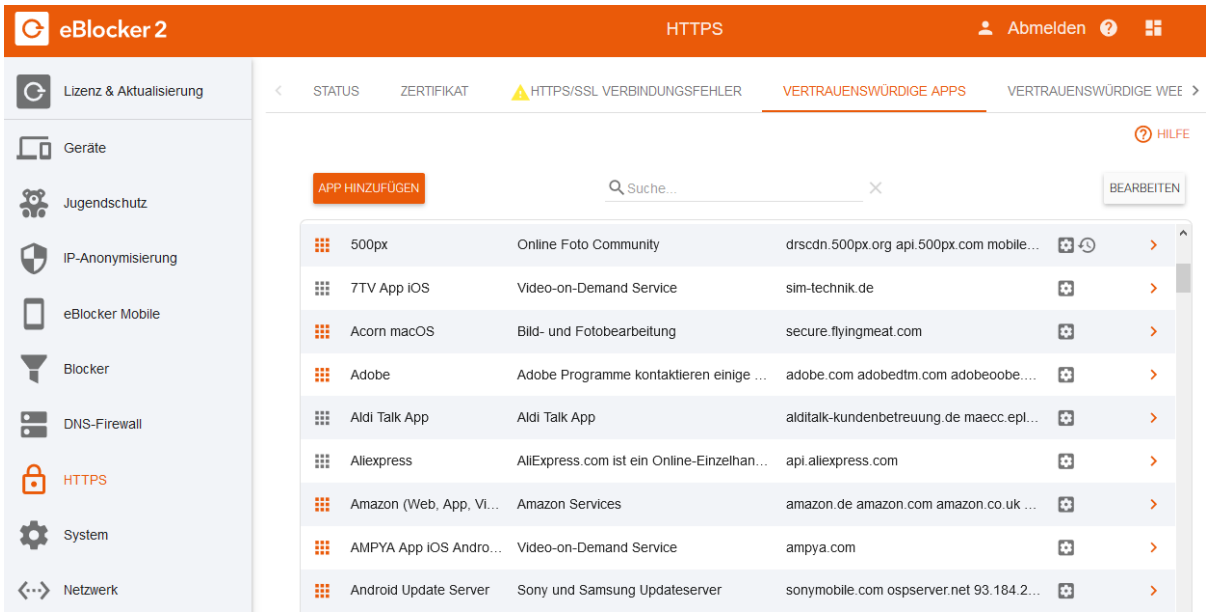
Hiermit fügen Sie die Domain zu der Liste der „Vertrauenswürdige Websites“ hinzu.

Mit dem Button „Alle Aufzeichnungen löschen“ wird die Liste der aktuell gefundenen Verbindungsfehlern gelöscht.

Tipp: Achten Sie bei den Namen der Domains auf den Namen der App, oder des Herstellers. Meist kann man so die gesuchte Verbindung schnell aufstöbern.

8.4.3 HTTPS - Vertrauenswürdige Apps

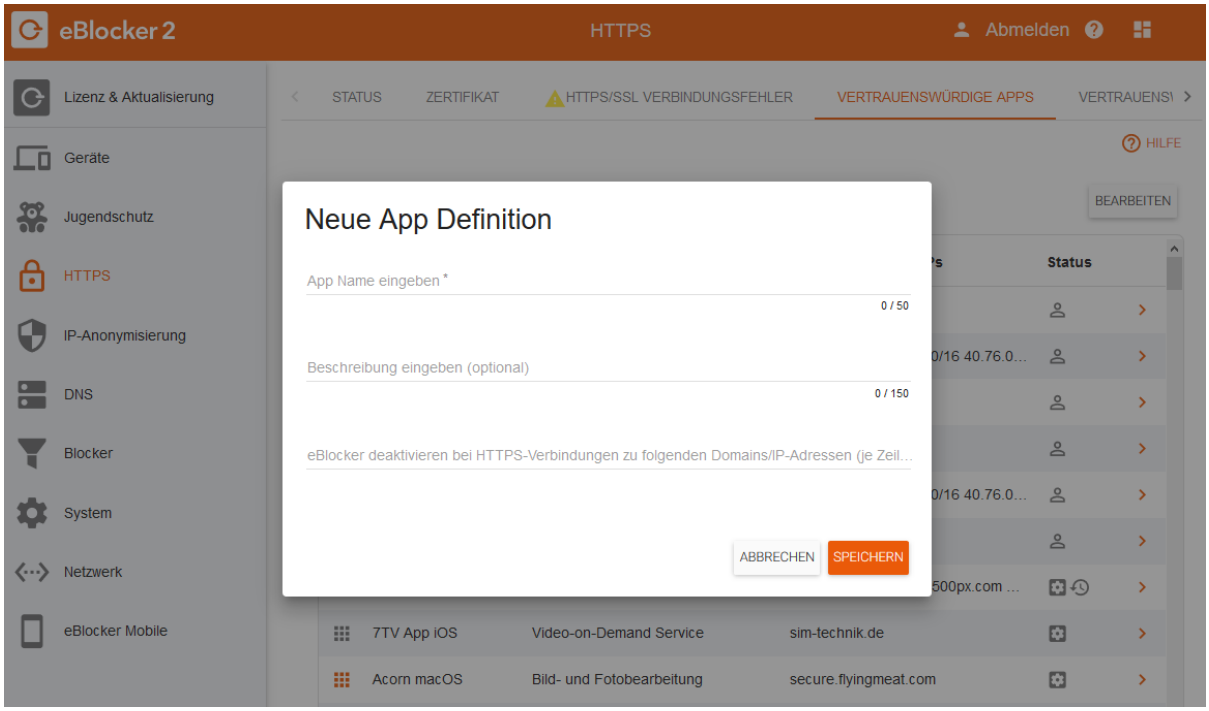
Falls einzelne Apps mit dem eBlocker nicht kompatibel sind, können Sie hier Websites, die von diesen Apps (oftmals unbemerkt im Hintergrund) angesprochen werden, vom Schutz durch den eBlocker ausnehmen.



Sie sehen hier eine Reihe von vordefinierten Ausnahmelisten für verschiedene Apps, die Sie nun mit einem Klick auf den Schiebeschalter auf der rechten Seite aktivieren oder deaktivieren können. Einige Ausnahmelisten für besonders populäre oder wichtige Apps sind bereits in der Grundeinstellung aktiviert.

Bitte beachten Sie, dass jede aktivierte Ausnahmeliste bedeutet, dass Sie auf den entsprechenden Websites nicht durch den eBlocker geschützt werden können. Ist für eine App, welche Sie suchen,

noch keine Ausnahmeliste definiert, können Sie diese über die Schaltfläche „Neue App definieren“ hinzufügen. Nach einem Klick auf die Schaltfläche erscheint ein neues Fenster.



Geben Sie den App-Namen ein und fügen Sie optional eine Beschreibung hinzu. Der App-Name muss eindeutig sein.

Geben Sie eine oder mehrere Domänen ein, die von der App verwendet werden, und die nicht vom eBlocker überwacht werden sollen. Geben Sie eine Domäne pro Zeile ein. Eine Zeile beenden Sie mit der Enter/Return-Taste.

Eine übergeordnete Domäne schließt dabei automatisch alle untergeordneten Domänen mit ein.

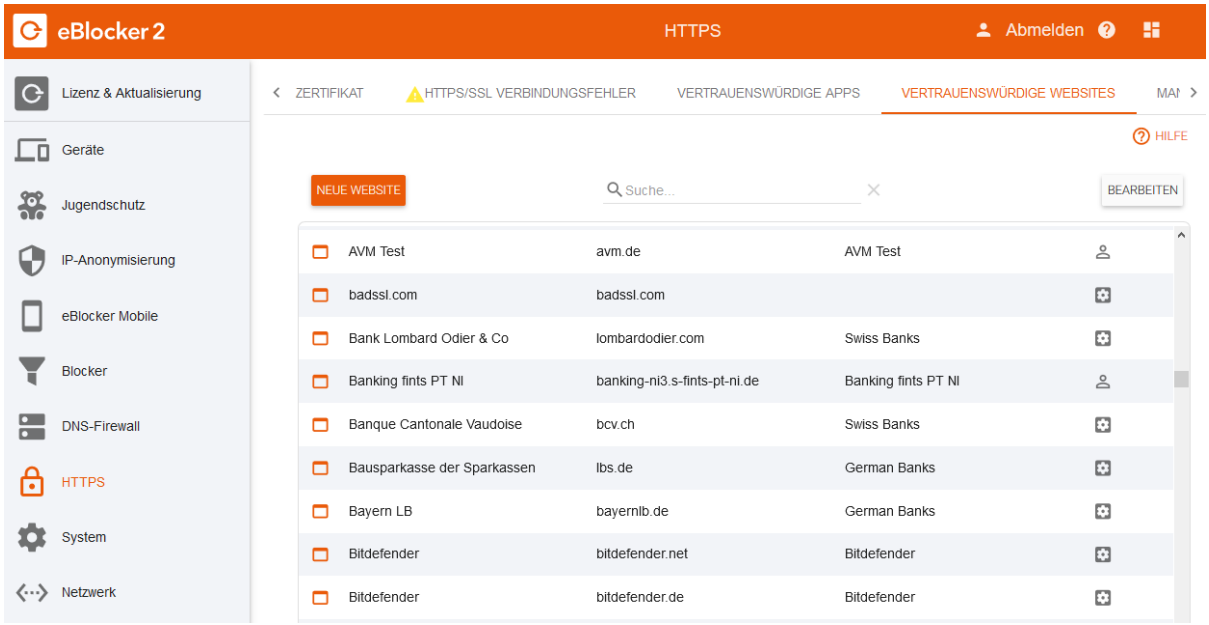
Beispiel: Wenn Sie die Domäne api.superapp.com auf die Ausnahmeliste setzen, dann werden automatisch auch Aufrufe zu Domänen wie login.api.superapp.com von der Überwachung durch den eBlocker ausgenommen.

In seltenen Fällen ist es nötig, IP-Adressen in die Ausnahmeliste aufzunehmen. IP-Adressen können Sie in das unterste Feld eingeben. Geben Sie wiederum eine IP-Adresse pro Zeile ein.

Schließen Sie den Vorgang ab, indem Sie auf „Speichern“ klicken. Ihre neue Ausnahmeliste wird dann gespeichert und gleich für Sie aktiviert.

8.4.4 HTTPS - Vertrauenswürdige Websites

Soll der eBlocker auf bestimmten, verschlüsselten Webseiten nicht aktiv werden, beispielsweise für Onlinebanking, können Sie die entsprechende Website auf der SSL-Ausnahmeliste hinzufügen.



Möchten Sie beispielsweise nicht, dass der eBlocker die SSL-Verbindungen zum Internet-Portal Ihrer Bank überwacht, so legen Sie einen entsprechenden Eintrag in der SSL-Ausnahmeliste an.

Wählen Sie einen eindeutigen Namen (z.B.: „Sparkasse Hamburg“), geben Sie die URL des Banking-Portals ein und schließen Sie den Vorgang ab, indem Sie den orangen Button mit der Aufschrift „Domain Hinzufügen“ betätigen.

Direkt unter den Eingabefeldern sehen Sie eine Ausnahmeliste, die bereits von uns vorbereitet wurde. Sind Sie mit einer der freigestellten Domains nicht einverstanden, können Sie diese bequem entfernen, indem Sie auf der rechten Seite auf die orange Mülltonne klicken. Sobald die Domain aus der Ausnahmeliste entfernt wurde, wird der eBlocker die Aufrufe an diese Website automatisch wieder überwachen, auch wenn die Verbindungen mit SSL verschlüsselt sind.

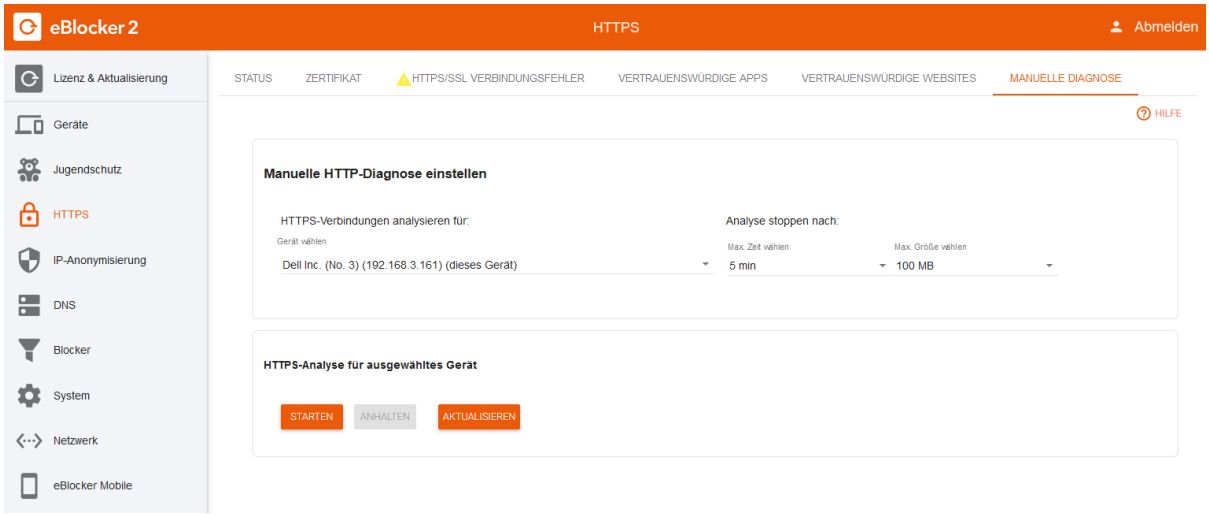
Wichtig: In dieser Ausnahmeliste sehen Sie auch die Domains der Ausnahmelisten der vertrauenswürdigen Apps. Diese können Sie hier nicht löschen.

8.4.5 HTTPS – Manuelle Diagnose

Gültig für eBlocker Pro und eBlocker Family

Die Manuelle Diagnose richtet sich in der aktuellen Version nur an technisch versierte Nutzer. Hiermit können Sie selbstständig untersuchen, warum ggf. einzelne Apps im Zusammenhang mit dem eBlocker nicht funktionieren (siehe auch Abschnitt 5.6). Mit entsprechender Definition von Ausnahmeregeln können Sie Probleme mit einzelnen Apps selbst beseitigen.

Gehen Sie dazu wie folgt vor: Analysieren Sie die von der App ausgehenden HTTPS-Verbindungen. Sie können dann Regeln festlegen, wie der eBlocker mit diesen Verbindungen umgehen soll (eBlocker für Verbindung aktivieren oder eBlocker für Verbindung deaktivieren). Wählen Sie dazu das Gerät, auf dem Sie die App verwenden, sowie die Dauer der Aufzeichnung und die maximale Größe der Aufzeichnungsdatei. Danach starten Sie die Aufzeichnung.



Verwenden Sie die App wie gewohnt. Testen Sie insbesondere die Funktionen, die nicht mit dem eBlocker kompatibel zu sein scheinen. Aktualisieren Sie die Liste der aufgezeichneten Verbindungen. Um die Domäne oder IP-Adresse zu finden, für die der eBlocker deaktiviert werden sollte, kann es notwendig sein, verschiedene Einstellungen auszuprobieren.

8.5 IP-Anonymisierung

Gültig für **eBlocker Base**, **eBlocker Pro** und **eBlocker Family**

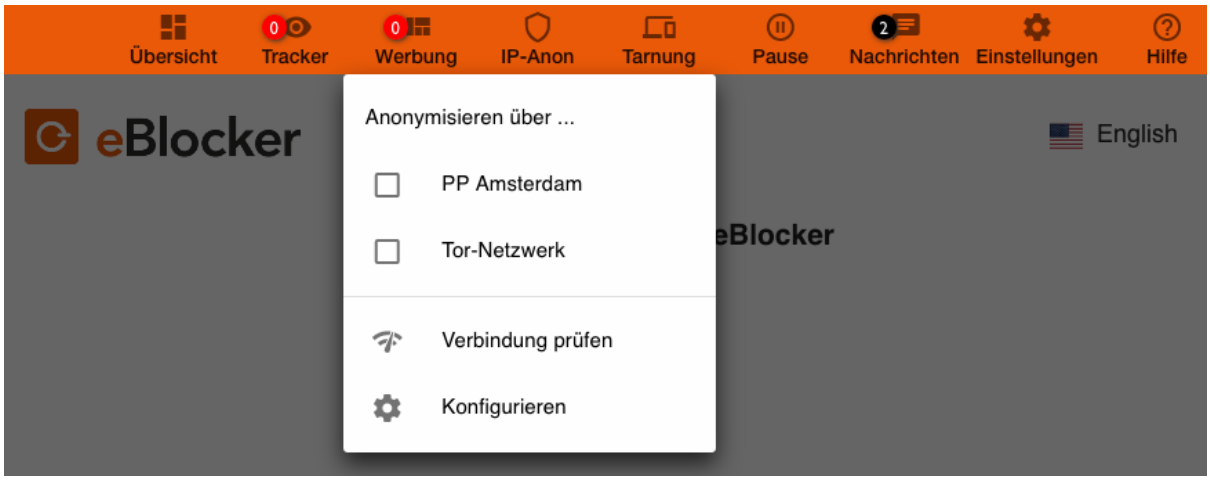
Wie in Abschnitt 7.5 erläutert, können Sie Ihre tatsächliche IP-Adresse durch Verwendung eines Anonymisierungsnetzwerks verschleiern.

8.5.1 Tor-Netzwerk einrichten und nutzen

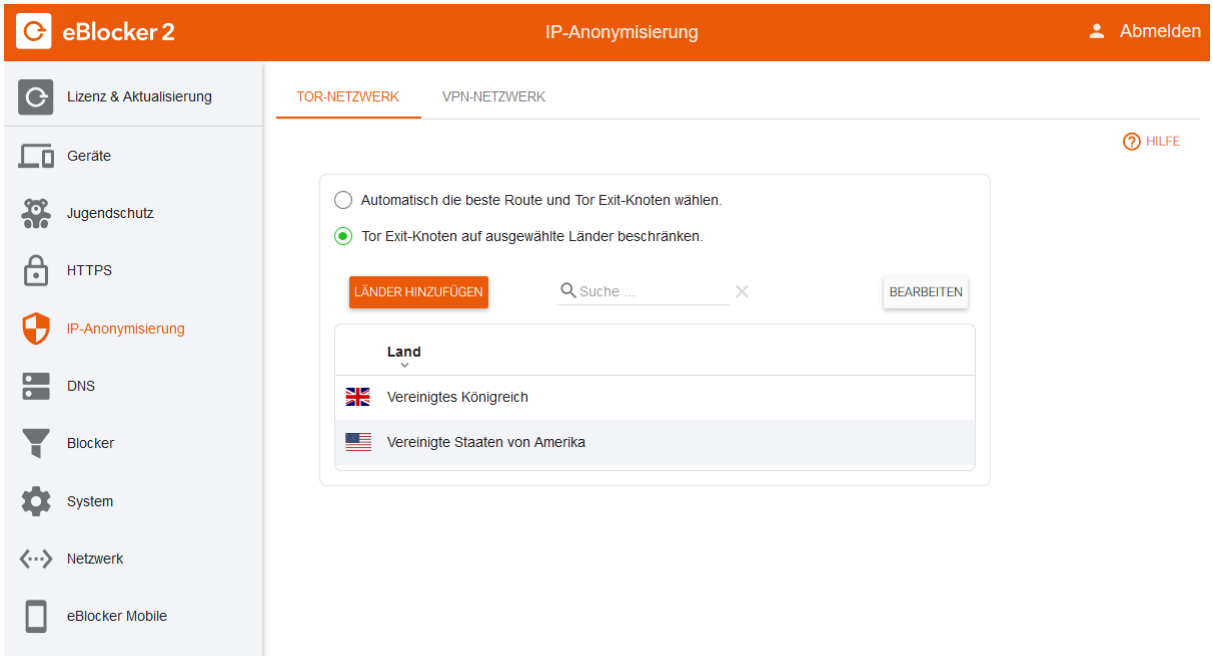
Gültig für **eBlocker Base**, **eBlocker Pro** und **eBlocker Family**

Der eBlocker verbindet sich zur IP-Anonymisierung standardmäßig immer über das Tor-Netzwerk.

Um die IP-Anonymisierung über das Tor-Netzwerk einzurichten und einzuschalten, öffnen Sie die Controlbar und klicken Sie auf „IP-Anon“. Wählen Sie "Konfigurieren", um zum Menü "IP-Anonymisierung" der eBlocker Einstellungen zu gelangen.



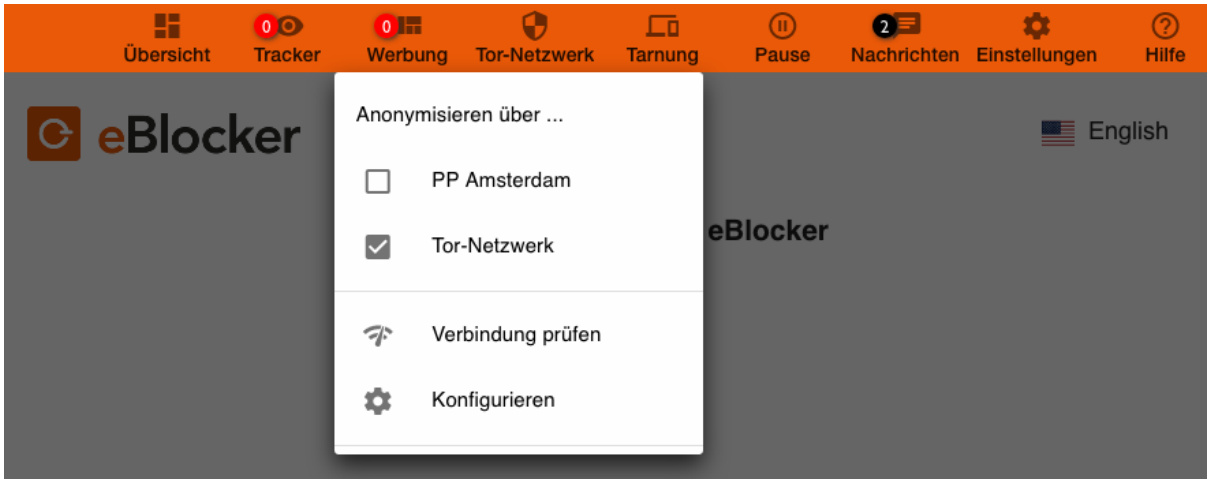
In den Einstellungen für das Tor-Netzwerk können Sie ein oder mehrere Länder auswählen, aus welchen Ihnen eine IP-Adresse zugewiesen wird.



Klicken Sie auf „Übernehmen“, um Ihre Auswahl zu bestätigen.

Rufen Sie jetzt eine beliebige Webseite auf, klicken auf das eBlocker Icon und öffnen die eBlocker Controlbar. Klicken Sie auf „IP-Anon“ und aktivieren Sie die Verbindung zum Tor-Netzwerk mit einem Klick „Tor-Netzwerk“.

Nach Aktivierung des Tor-Netzwerks, wird das IP-Anon-Symbol zusätzlich in der Controlbar mit einem Karomuster ausgefüllt, um zu signalisieren, dass die IP-Anon-Funktion aktiv ist. Fortan werden sämtliche HTTP-Anfragen durch ein Anonymisierungsnetzwerk geleitet. Ist SSL/HTTPS auf dem eBlocker aktiviert, werden auch HTTPS-Anfragen durch ein Anonymisierungsnetzwerk geleitet.



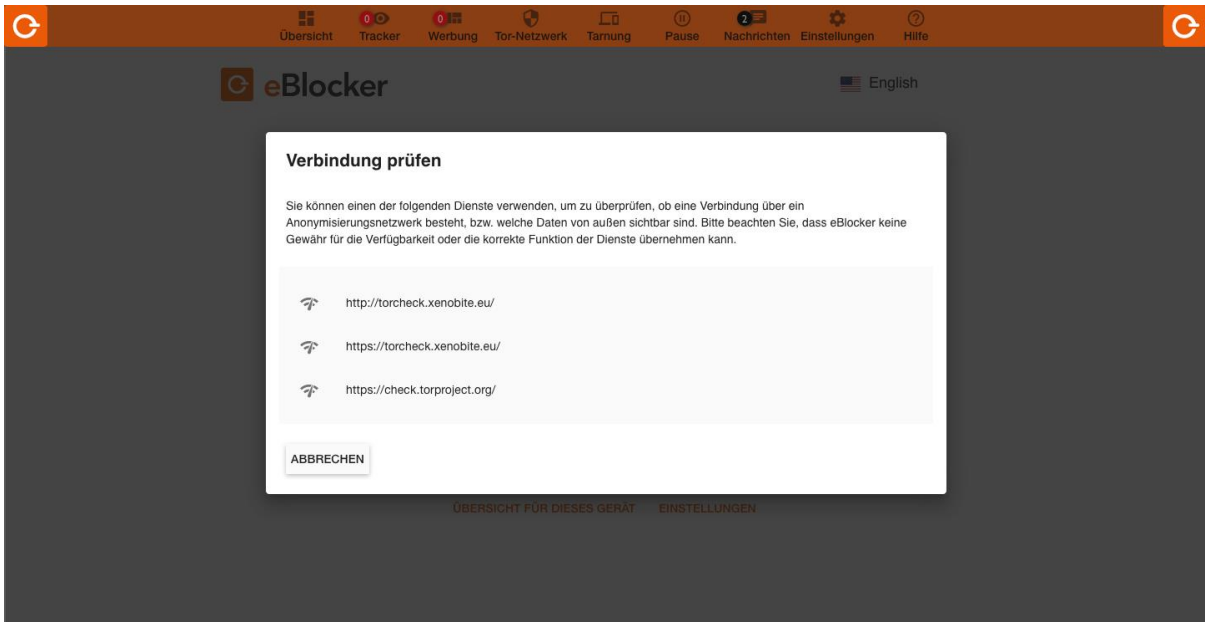
Ab sofort surfen Sie anonym über die Ihnen durch das Tor-Netzwerk zugewiesene IP-Adresse. Für einen Internet-Dienstanbieter erscheint es, als ob Sie aus einem der von Ihnen gewählten Länder

kommen. So können Sie Zensur umgehen oder auf Inhalte zugreifen, die nur in bestimmten Regionen der Welt verfügbar sind.

Bitte beachten Sie, dass das Tor-Netzwerk ein Verbund freiwilliger Internet-Aktivisten ist, die den Service kostenfrei aber ohne Verfügbarkeitsgarantie bereitstellen. Nicht in allen Ländern gibt es aktive Ausgangsserver, sodass Sie ggf. Ihre Wahl ändern oder erweitern müssen, um Tor nutzen zu können.

Wenn kein Land ausgewählt ist, wird ein Ausgangsserver aus einem beliebigen Land verwendet.

Mit einem Klick auf "Verbindung prüfen" können Sie prüfen, ob nach der Aktivierung vom Tor-Netzwerk eine Verbindung zum Tor-Netzwerk besteht. Dazu haben wir Ihnen drei der bekannten Webseiten ausgesucht.



Mit einem Klick auf "Tor: Neue Identität beziehen" können Sie aus der Controlbar zu einem anderen Tor-Ausgangsserver aus dem Land wechseln.

Um die Tor-Verbindung wieder zu trennen, klicken Sie erst auf das "IP-Anon"-Symbol und dann auf das "Tor-Netzwerk". Das Karomuster im Anon-Symbol in der Controlbar wird nicht mehr angezeigt.

8.5.2 Alternatives VPN-Netzwerk einrichten

Gültig für **eBlocker Base**, **eBlocker Pro** und **eBlocker Family**

Anstelle des standartmäßig über den eBlocker zur Verfügung gestellten Tor-Netzwerks können Sie eine VPN-Verbindung eines beliebigen anderen VPN-Anbieters nutzen.

Eine VPN-Verbindung richten Sie im Menü „VPN-Netzwerke" ein. Das Menü finden Sie unter „eBlocker Einstellungen > IP-Anonymisierung". Dort finden Sie auch einen Link zur Liste mit den von uns getesteten VPN-Anbietern, die stets erweitert wird. Sie können auch andere VPN-Anbieter nutzen, solange diese Anbieter das OpenVPN-Protokoll unterstützen.

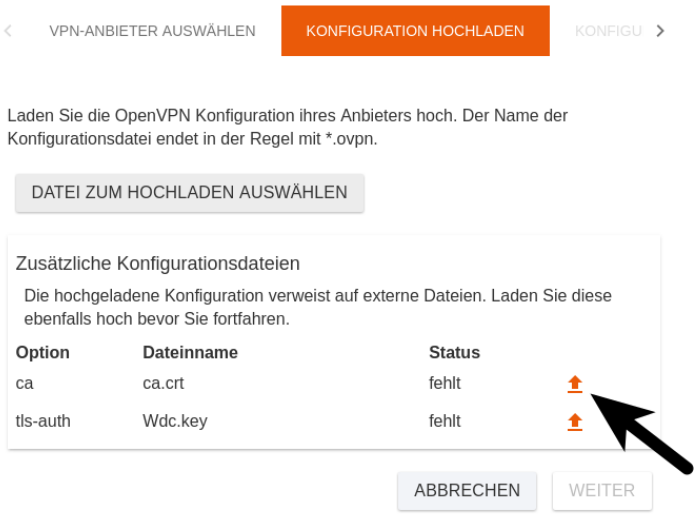
Achtung:
Durch die Nutzung der Services von VPN-Anbietern können Ihnen zusätzliche Kosten entstehen. Die Verbindungsgeschwindigkeit kann ggf. vom VPN-Anbieter abhängig sein.

Von Ihrem VPN-Anbieter werden Ihnen ein Benutzernamen, ein Passwort und eine Konfigurationsdatei mit der Endung ".ovpn" bereitgestellt. Diese Konfigurationsdatei ist nötig, um die Verbindung zum VPN-Netzwerk einzurichten.

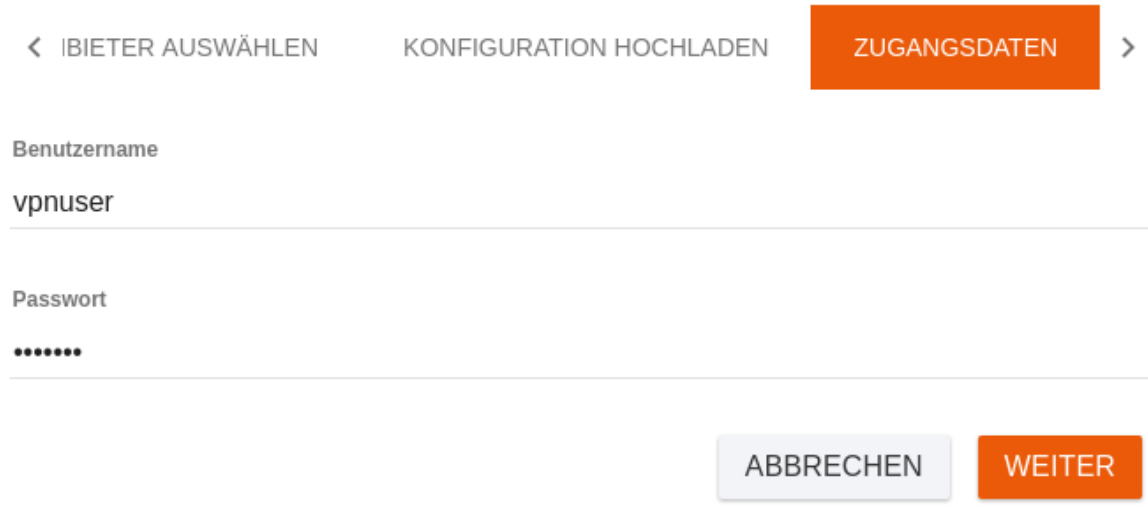
Um eine VPN-Verbindung herzustellen, legen Sie zunächst einen neuen VPN-Anbieter an. Klicken Sie hierzu auf „Neuer VPN-Anbieter".

Folgen Sie nun den Anweisungen des Assistenten und laden Sie die von Ihrem VPN-Anbieter bereitgestellte Konfigurationsdatei hoch.

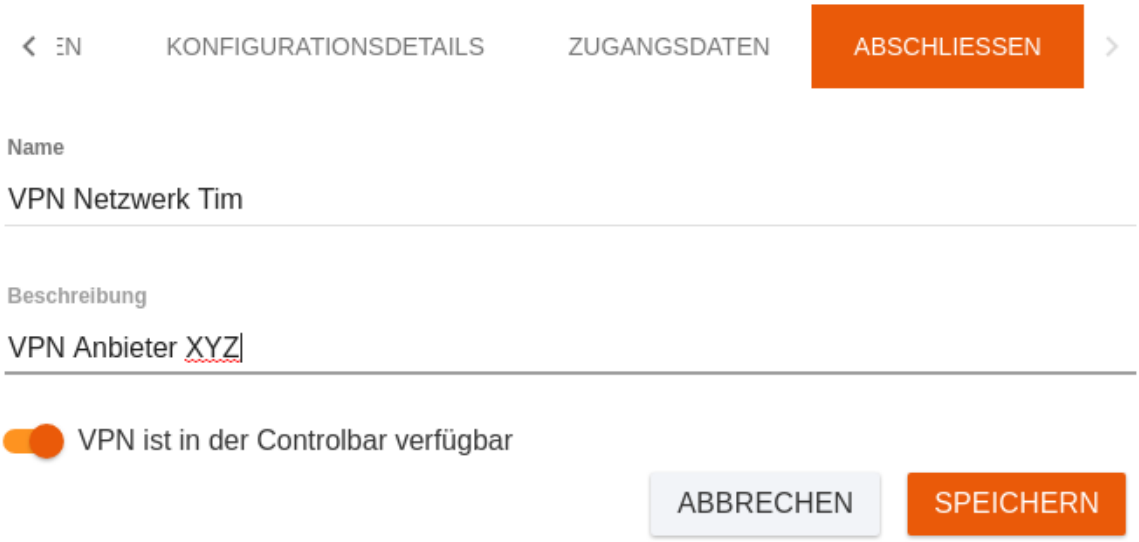
Nach dem Hochladen der Konfigurationsdatei haben Sie ggf. noch die Möglichkeit weitere Dateien hoch zu laden. Anschließend werden Ihnen einige Informationen angezeigt. Dabei handelt es sich zum Beispiel um ignorierte oder nicht unterstützte Optionen vom eBlocker, die in der Regel unbedenklich sind und zu keiner Funktionsstörung führen. Der eBlocker kann auch weiterhin optimal genutzt werden. Klicken Sie auf "Weiter".



Geben Sie unter „Zugangsdaten“ Benutzernamen und Passwort ein, die Sie von Ihrem VPN-Anbieter erhalten haben. Klicken Sie dann auf „Weiter".

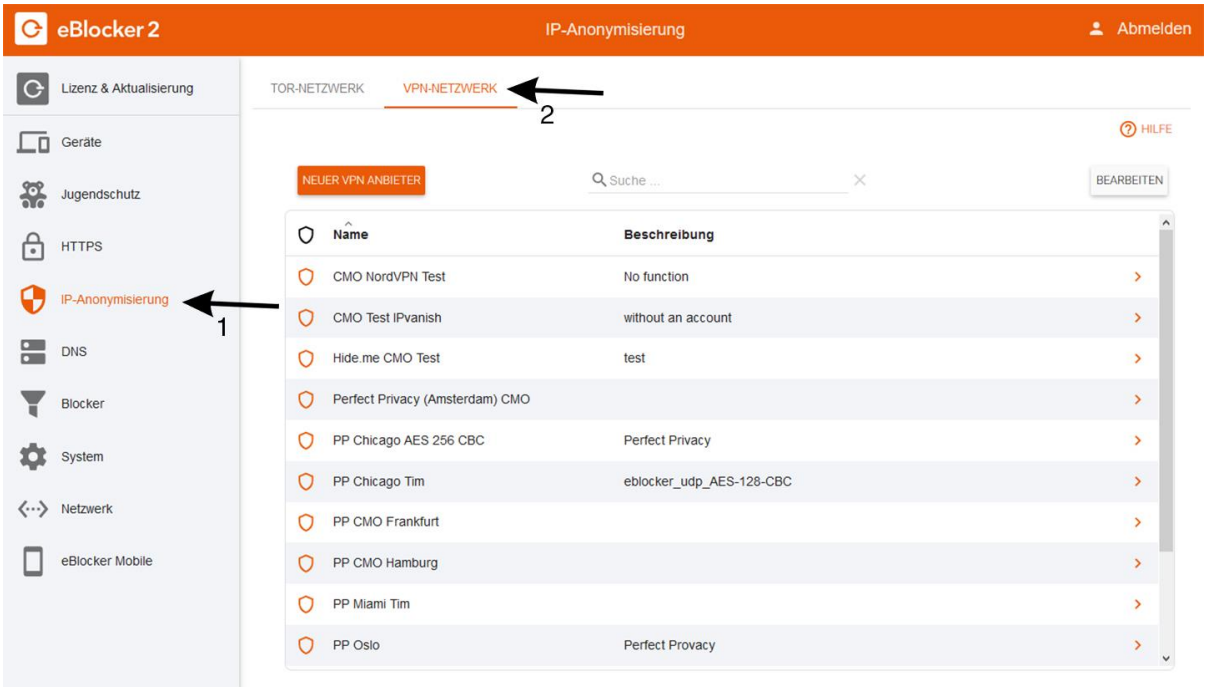


Vergeben Sie anschließend für dieses VPN-Netzwerk einen Namen und eine Beschreibung. Legen Sie abschließend fest, ob das VPN-Netzwerk in der Controlbar verfügbar sein soll. Soll die Verbindung nicht in der Controlbar angezeigt werden, wird sie in Ihren Einstellungen lediglich als inaktiv angezeigt.



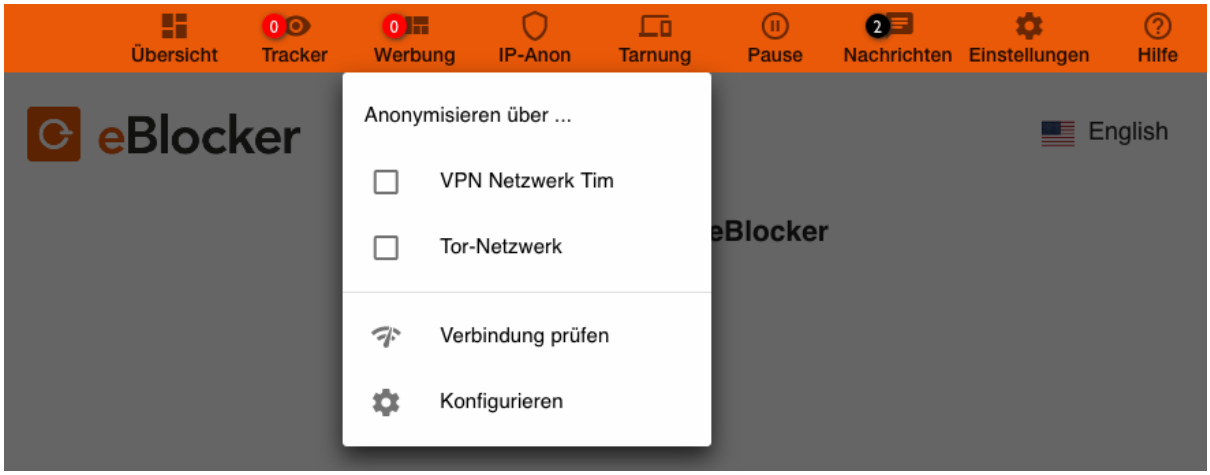
Sie haben erfolgreich ein neues VPN-Netzwerk angelegt und können dieses mit einem Klick auf den Namen ggf. bearbeiten oder entfernen oder einen Verbindungstest ausführen.

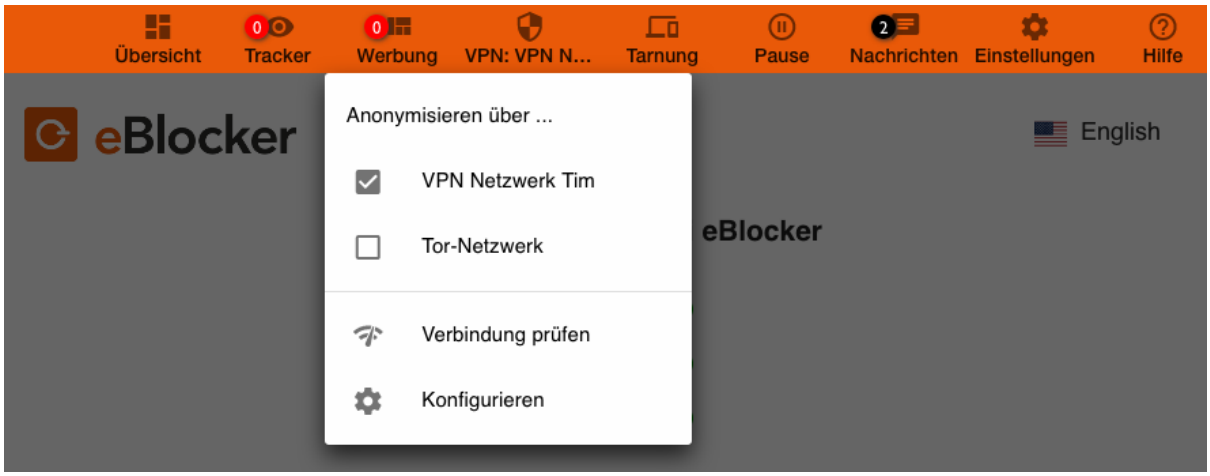
In der eBlocker Controlbar sehen Sie unter dem Menüpunkt „Anon" das soeben angelegte VPN-Netzwerk. Mit einem Klick auf das VPN-Netzwerk wird zuerst die Verbindung geprüft.



Die erfolgreiche Verbindung zum VPN-Netzwerk wird danach mit einem Häkchen angezeigt. Sollte Sie nicht erfolgreich sein, wird kein Haken angezeigt. Gehen Sie hierfür in Ihre Einstellungen zurück und prüfen Sie Ihren Benutzernamen und Passwort.

Nach Aktivierung des VPN-Netzwerks wird das Anon-Symbol zusätzlich in der Controlbar mit einem Karomuster ausgefüllt, um zu signalisieren, dass die Anon-Funktion aktiv ist.





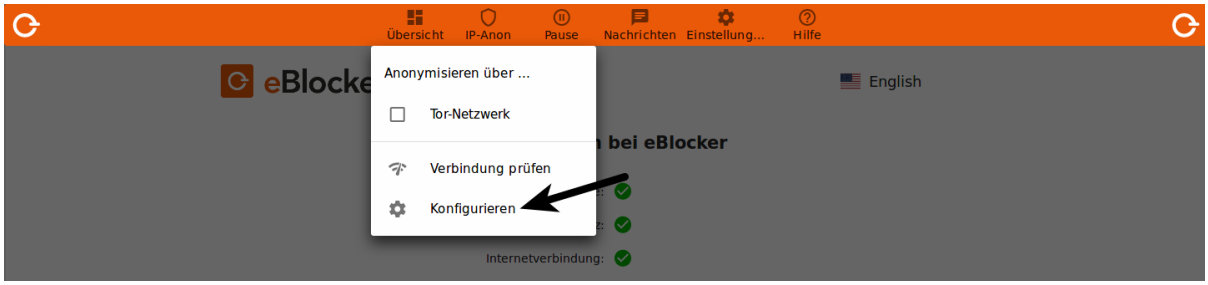
Um die VPN-Verbindung wieder zu trennen, klicken Sie erst auf das Anon-Symbol und dann auf das VPN-Netzwerk. Das Anon-Symbol in der Controlbar zeigt wieder ein nicht ausgefülltes Karomuster.

Achtung:

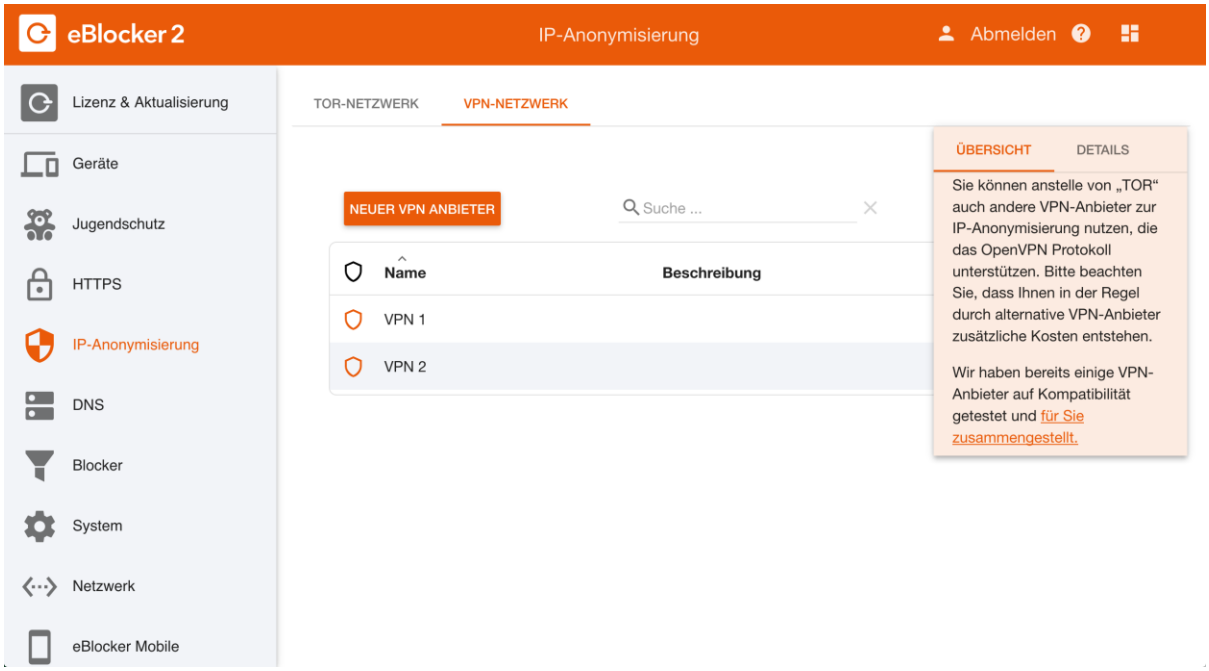
Eine Tor-Vorbindung kann nicht zeitgleich mit einer bestehenden VPN- oder einer anderen bestehenden Tor-Verbindung genutzt werden.

8.5.3 VPN-Netzwerk für eBlocker Base einrichten

Öffnen Sie die eBlocker Controlbar durch einen Klick auf das eBlocker Icon. Klicken Sie nun auf das Icon „IP-Anon“. Es öffnet sich ein Pulldown-Menue. Klicken Sie auf „Konfigurieren“.



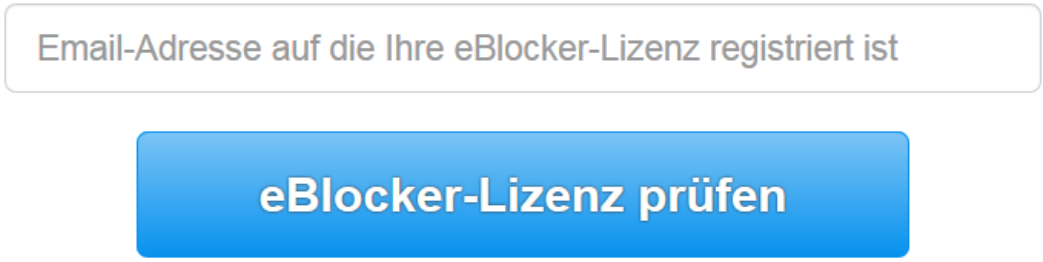
Es öffnet sich eine neue Seite. Klicken Sie auf den Reiter „VPN-Netzwerk“ und rechts auf den Link „Übersicht“. Es öffnet sich ein kleines Fenster mit einem Link einiger VPN-Anbieter, die wir auf Kompatibilität für Sie getestet und zusammengestellt haben.



Sie gelangen nun auf die Seite, auf der die von uns getesteten VPN-Netzwerke aufgelistet sind. Klicken Sie auf „Perfect Privacy“.

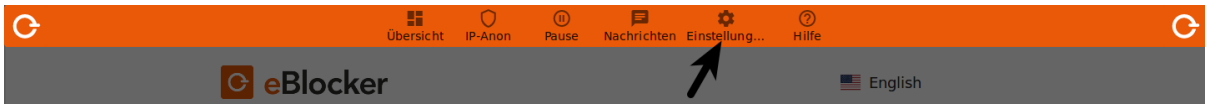
Sie befinden sich jetzt auf der Seite von Perfect Privacy.

Scrollen Sie auf dieser Seite nach unten. Geben Sie im Freifeld exakt die E-Mail-Adresse ein, mit der Sie Ihren eBlocker registriert haben. Klicken Sie auf das blaue Feld „eBlocker Lizenz prüfen“.



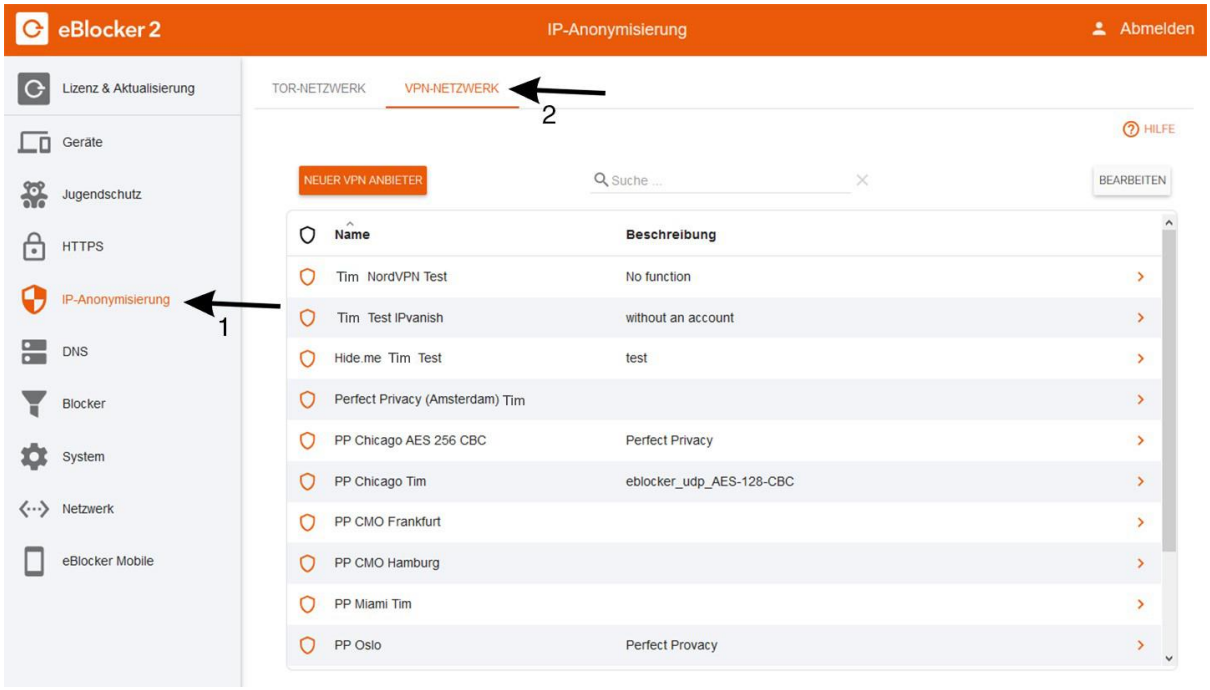
Von Ihrem VPN-Anbieter werden Ihnen ein Benutzernamen, ein Passwort und eine Konfigurationsdatei mit der Endung ".ovpn" bereitgestellt. Diese Konfigurationsdatei ist nötig, um die Verbindung zum VPN-Netzwerk einzurichten. Laden Sie die Konfigurationsdatei herunter und merken sich bitte den Ort, wohin Sie diese Datei speichern.

Öffnen Sie nun bitte erneut die eBlocker-Controlbar und klicken auf das Icon „Einstellungen“.

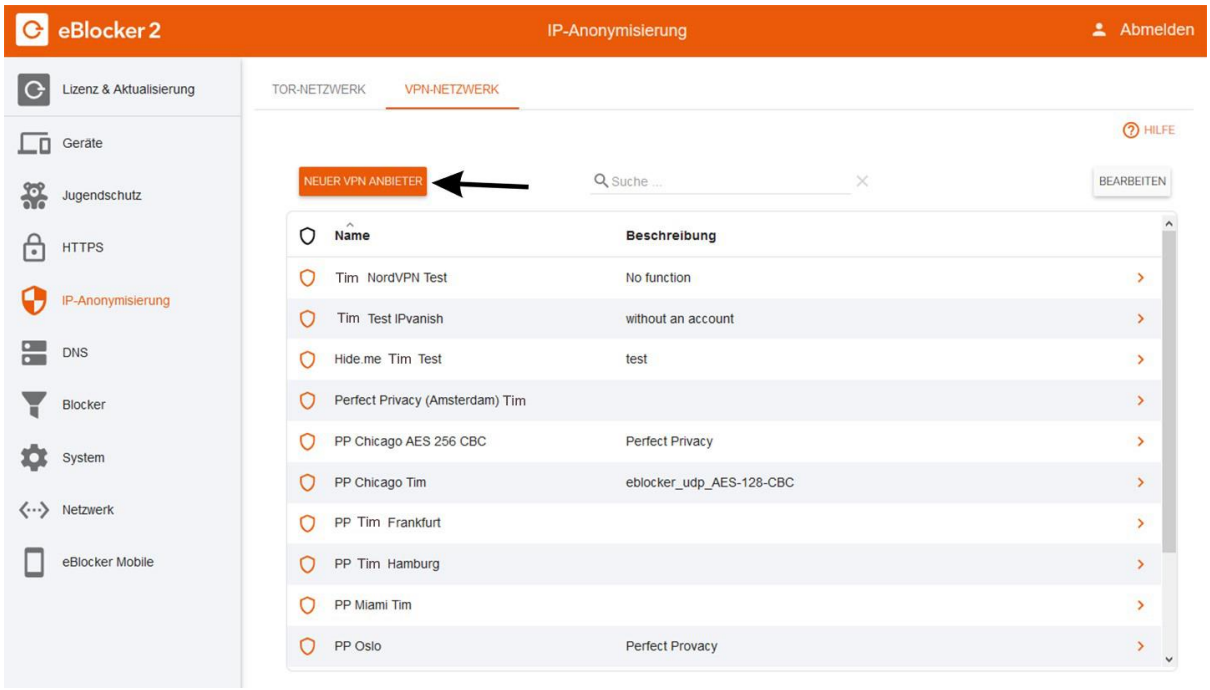


Auf der sich öffnenden Seite klicken Sie ganz links bitte auf „IP-Anonymisierung“.

Auf der rechten Seite wechselt der Inhalt. Klicken Sie dort bitte oben auf „VPN-Netzwerk“.

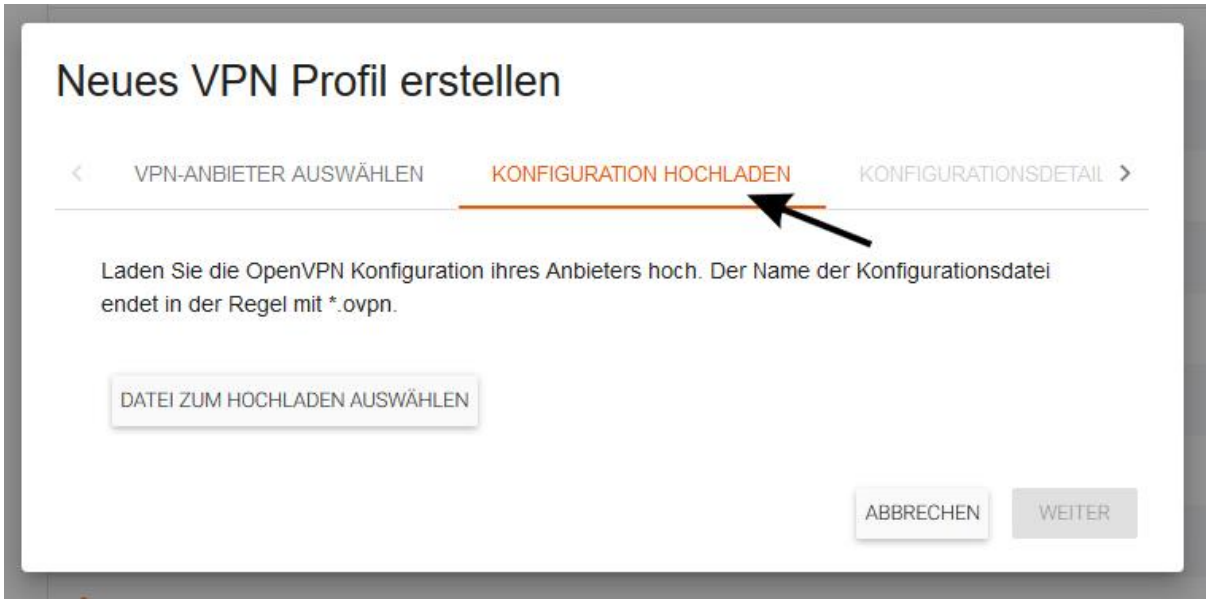


Klicken Sie nun auf den Button „Neuer VPN-Anbieter“.



Es öffnet sich ein PopUp-Fenster. Dieser Wizard unterstützt Sie bei der Einrichtung von VPN.

Klicken Sie bitte im Fenster auf „Konfiguration hochladen“ und laden Sie Ihre Datei hoch.



Nach dem Hochladen der Konfigurationsdatei haben Sie ggf. noch die Möglichkeit weitere Dateien hoch zu laden. Anschließend werden Ihnen einige Informationen angezeigt. Dabei handelt es sich zum Beispiel um ignorierte oder nicht unterstützte Optionen vom eBlocker, die in der Regel unbedenklich sind und zu keiner Funktionsstörung führen. Der eBlocker kann auch weiterhin optimal genutzt werden. Klicken Sie auf "Weiter".

*Geben Sie unter „*Zugangsdaten“ Benutzernamen und Passwort ein, die Sie von Ihrem VPN-Anbieter erhalten haben. Klicken Sie dann auf „Weiter".

Vergeben Sie anschließend für dieses VPN-Netzwerk einen Namen und eine Beschreibung. Legen Sie abschließend fest, ob das VPN-Netzwerk in der Controlbar verfügbar sein soll.

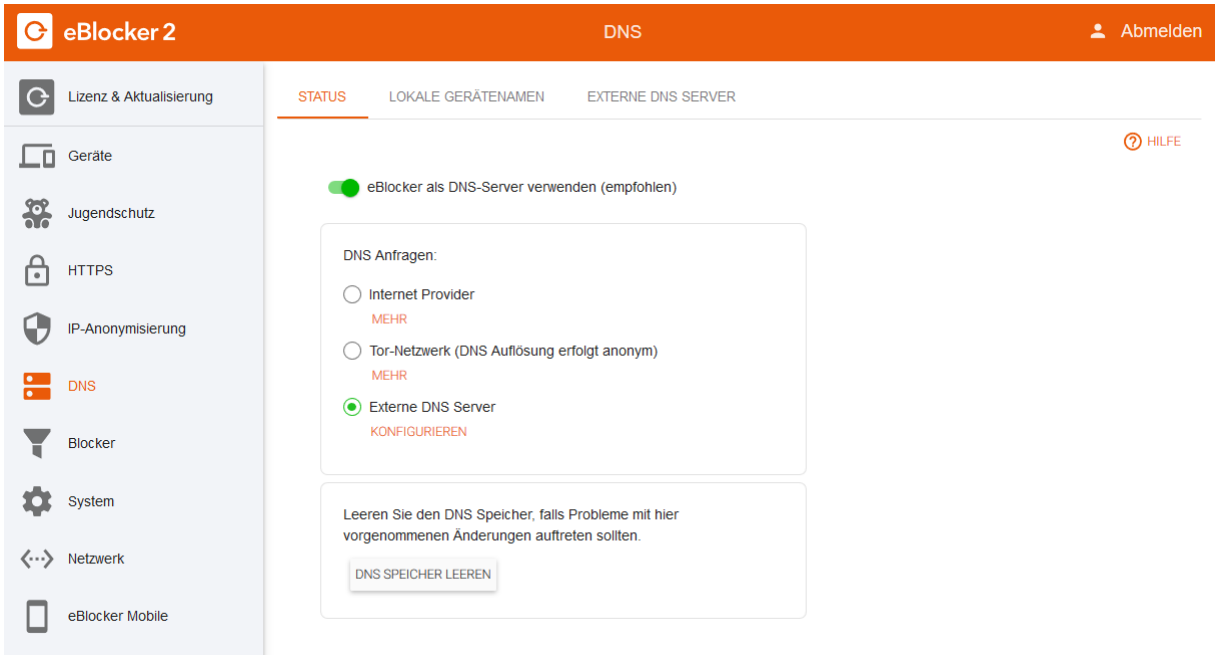
Schließen Sie den Vorgang mit „Abschließen“ ab. Sie sind nun über das VPN-Netzwerk Perfect Privacy anonym im Netz unterwegs und haben sich **3 Monate kostenlosen VPN Service** gesichert.

In der eBlocker Controlbar sehen Sie unter dem Menüpunkt „Anon" das soeben angelegte VPN-Netzwerk. Mit einem Klick auf das VPN-Netzwerk wird zuerst die Verbindung geprüft.

Die erfolgreiche Verbindung zum VPN-Netzwerk wird danach mit einem Häkchen angezeigt. Sollte Sie nicht erfolgreich sein, wird kein Haken angezeigt. Gehen Sie hierfür in Ihre Einstellungen zurück und prüfen Sie Ihren Benutzernamen und Passwort.

Der VPN-Dienst ist für jedes Endgerät individuell aktivierbar.

8.6 DNS



Wenn Sie diese Funktion aktivieren, können Sie die DNS Anfragen über Ihren eBlocker an eine Liste von verschiedenen DNS Servern verteilen oder über des Tor-Netzwerks auflösen lassen. Ihnen stehen dafür drei verschiedene Optionen zur Verfügung.

- Internet Provider
- Tor-Netzwerk (DNS Auflösung erfolgt anonym)
- Externe DNS Server

Internet Provider

Hier wird der DNS Server verwendet, welchen Sie in Ihrer Router Konfiguration hinterlegt haben.

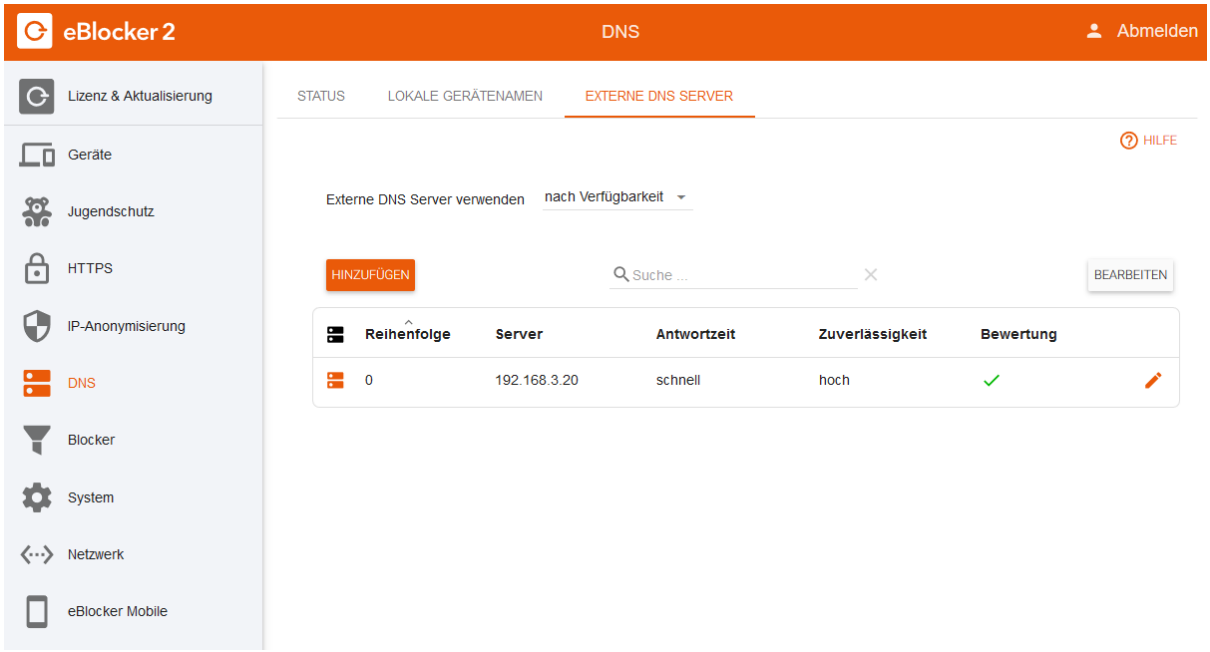
Tor-Netzwerk (DNS Auflösung erfolgt anonym)

Hier werden die DNS Anfragen durch das Tor-Netzwerk geleitet und am Ausgangspunkt des Tor-Netzwerkes an einen DNS Server übergeben. Vergewissern Sie sich, dass Tor verfügbar ist. Dies können Sie im Menü IP-Anonymisierung > Tor-Netzwerk überprüfen.

Die DNS-Funktion sollte derzeit nicht genutzt werden, wenn sie einen eigenen DNS-Server im lokalen Netz betreiben. Es kann sonst zu Problemen beim Auflösen von internen oder externen IP-Adressen führen.

Externe DNS Server

Mit dieser Option können Sie eine Liste von DNS Servern hinterlegen. Diese Liste kann nach Verfügbarkeit, der Reihe nach oder in zufälliger Reihenfolge vom eBlocker abgearbeitet werden. Die einzelnen DNS Server können Sie im Reiter „DNS Server Liste“ anlegen.

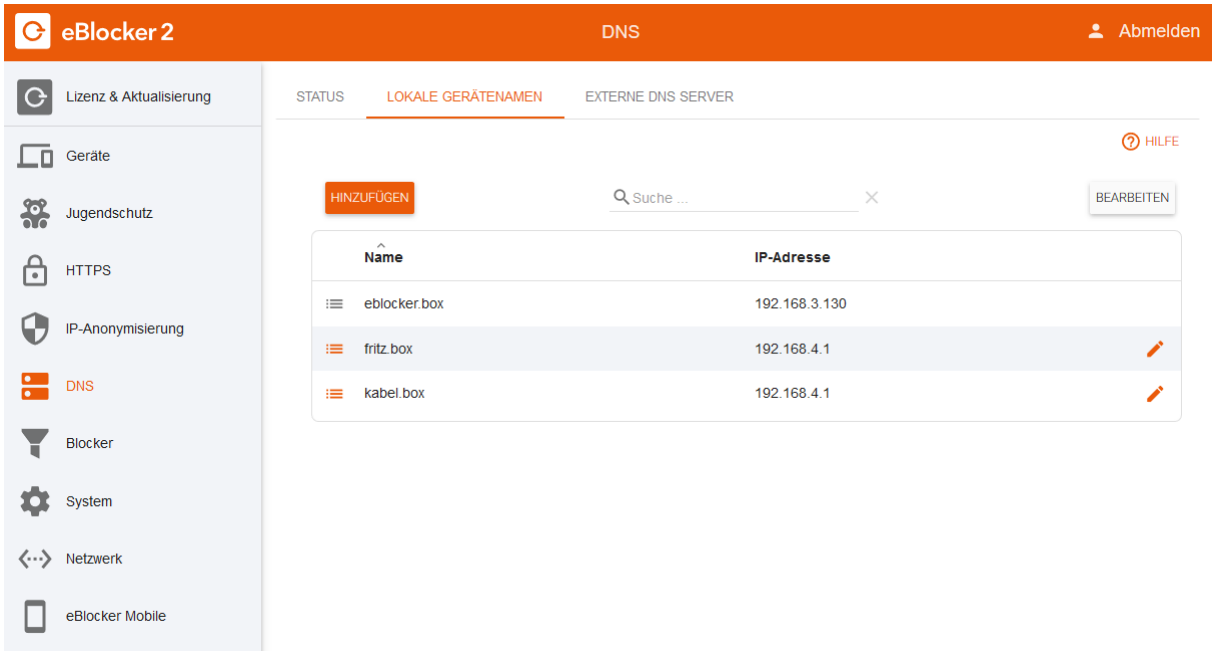


8.6.1 DNS – Lokale Gerätenamen

Hier können Sie für Ihr Netzwerk bestimmten IP-Adressen, einen Servernamen zuordnen.

Beispiel: Wenn Sie eine Fritzbox einsetzen, werden Sie bemerkt haben, dass Sie bei aktivierter eBlocker DNS Funktion, „fritz.box“ im Browser nicht mehr aufrufen können. Das liegt daran, dass der DNS Server vom eBlocker und nicht mehr von der Fritzbox benutzt wird. Der eBlocker erkennt die „fritz.box“ nicht.

Klicken Sie auf den Button „Hinzufügen“ und vergeben Sie einen Servernamen wie zum beispiel fritz.box. Geben Sie nun im Feld IP-Adresse die IP-Adresse Ihrer Fritzbox ein (Beispiel: 192.168.178.1). Nun klicken Sie auf den Button „Speichern“ und Sie sehen einen neuen Eintrag in der Liste.



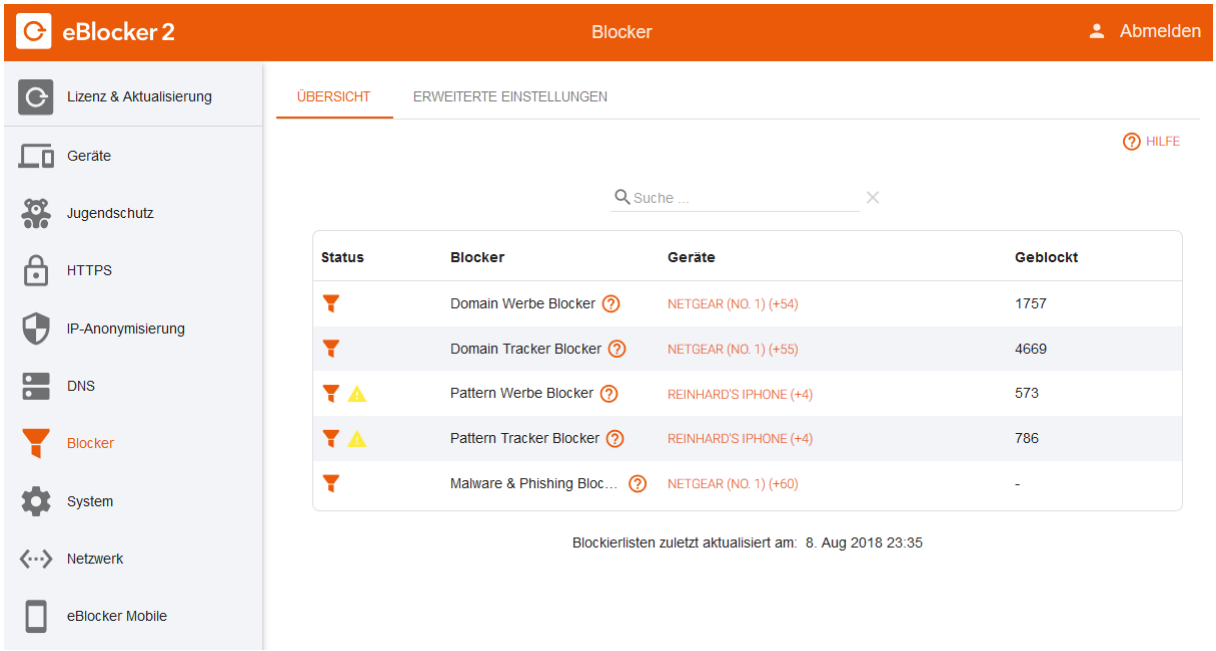
Wenn Sie nun in einem Browser fritz.box eingeben, können Sie die Einstellungen Ihrer Fritzbox wieder erreichen.

8.7 Blocker

Hier erhalten Sie eine Übersicht über die vom eBlocker verwendeten Blocker und können zudem weitere Einstellungen aktivieren.

8.7.1 Blocker – Übersicht

Hier erhalten Sie eine Übersicht über die genutzten Blocker Funktionen des eBlocker. Wenn Sie mit der Maus über die einzelnen Symbole fahren, erhalten Sie weitere Informationen.



Status

Fahren Sie mit der Maus über das Status Symbol und Sie bekommen eine kurze Information zu dem Filter und die Anzahl der Geräte, welche diesen Blocker benutzen.

Sehen Sie hier hinter dem Status Symbol ein gelbes Dreieck, so ist das ein extra Hinweis zu dem Blocker. Wenn Sie mit der Maus über das gelbe Dreieck fahren, wird Ihnen der Hinweis angezeigt.

Blocker

Es gibt drei Blocker Funktionen.

- Die Domain Blocker für Werbung und Tracker blockieren schon beim Aufrufen der Domain, Werbungen und Tracker. Dieser Blocker kann auch ohne die Aktivierung der eBlocker HTTPS Funktion genutzt werden.
- Die Pattern Blocker für Webung und Tracker erkennen anhand von Mustern die Tracker und Werbung. Für diese Blocker ist die Aktivierung von der eBlocker SSL Funktion notwendig.
- Malware und Phishing Blocker Geräte

Hier sehen Sie eine Auflistung alle Geräte, welche diesen Blocker zurzeit nutzen. Wenn Sie mit der Maus über die Gräte fahren, wird eine Liste mit allen Geräten angezeigt.

Blockierte Anfragen

Hier sehen Sie eine Auflistung aller blockierten Anfragen von allen Geräten seit dem Start Ihres eBlockers.

8.7.2 Blocker – Erweiterte Funktionen

Gültig für **eBlocker Pro** und **eBlocker Family**

8.7.3 Captive Portal Check

Google Captive Portal Check wird von Google-Produkten wie Android, Chrome und Chromebooks benutzt um zu testen, ob eine Internet-Verbindung besteht. Dabei wird Ihre IP-Adresse zum Google Captive Portal gesendet. eBlocker blockiert den Aufbau zum Google Captive Portal, da sonst Ihre IP-Adresse von Google erfasst wird. Aktivieren Sie diese Option mit einem Klick, wenn Android-Geräte oftmals von Ihrem WLAN getrennt werden.

8.7.4 Do Not Track

Do-Not-Track (DNT) ist ein HTTP-Header-Feld, welche einer Website signalisiert, dass der Besucher kein Nutzerprofil von der Website erstellt haben möchte. Leider ist dieser Wunsch des Benutzers unverbindlich und wird daher von sehr vielen Websites nicht beachtet.

Bei den meisten Browsern ist diese Funktion in den Einstellungen zum Datenschutz oder zur Sicherheit zu finden.

Der eBlocker macht es Ihnen leichter und setzt nach Aktivierung der Funktion das Do-Not-Track Feld automatisch in allen Anfragen.

8.7.5 HTTP Referrer Header

HTTP Referrer Header werden automatisch erstellt, wenn Sie im Internet surfen. Der Referrer zeigt die Webseite an, die Sie besucht haben bevor Sie auf die aktuelle Webseite gelangt sind.

Durch Nutzung der Referrer-Header können Websites Ihre Surfgewohnheiten teilweise verfolgen. Einige Webseiten nutzen die Referrer-Header auch für interne Zwecke. Das Blockieren der Referrer-Header kann daher dazu führen, dass einige Seiten nicht mehr richtig angezeigt werden. Entscheiden Sie mit einem Klick, ob Referrer-Header zugelassen werden sollen.

8.7.6 Kompression

Webserver komprimieren oftmals die ausgelieferten Webseiten, um die übertragene Datenmenge im Internet möglichst gering zu halten. Der eBlocker muss dann die Daten dekomprimieren, um die Seite analysieren und seine Schutzfunktionen ausführen zu können. In Ihrem lokalen Netzwerk würde sich durch eine erneute Kompression auf dem letzten Stück zum Gerät kein Geschwindigkeitsvorteil ergeben. Im Gegenteil: Der Seitenaufbau ist in der Regel sogar schneller, wenn für dieses letzte Stück auf eine erneute Kompression und Dekompression verzichtet wird.

Nur wenn Ihr Gerät von unterwegs über eBlocker Mobile verbunden ist, sollte eine Kompression zum Gerät erfolgen.

Daher bietet die Kompressionsfunktion des eBlockers Ihnen drei Einstellungen.

8.7.7 Keine Kompression

Hier werden die Daten für den kurzen Weg zwischen eBlocker und Gerät nicht wieder komprimiert.

8.7.8 Kompression für eBlocker Mobile Geräte (empfohlen)

Auch hier werden die Daten für den kurzen Weg zwischen eBlocker und Gerät nicht wieder komprimiert. Nur wenn Ihr Gerät sich von unterwegs über eBlocker Mobile verbindet, werden die Daten zwischen eBlocker und Gerät komprimiert.

8.7.9 Immer komprimieren

Hier werden die Daten beim Transport vom eBlocker zum Gerät grundsätzlich komprimiert.

8.7.10 WebRTC

WebRTC ist eine Browser-Technologie, mit der Kommunikation zwischen zwei Parteien in Echtzeit ermöglicht wird. Sie wird beispielsweise für Internet-Telefonie und Chat verwendet.

Leider offenbart WebRTC Ihre echte IP-Adresse (und sogar Ihre lokale LAN-IP), um die Verbindungen herzustellen. Selbst bei der Verwendung von Tor (IP-Anonymisierung), können Sie so über Ihre echte IP-Adresse identifiziert werden, wenn WebRTC nicht blockiert wird. Entscheiden Sie mit einem Klick, ob WebRTC-Verbindungen zugelassen werden sollen.

8.8 System

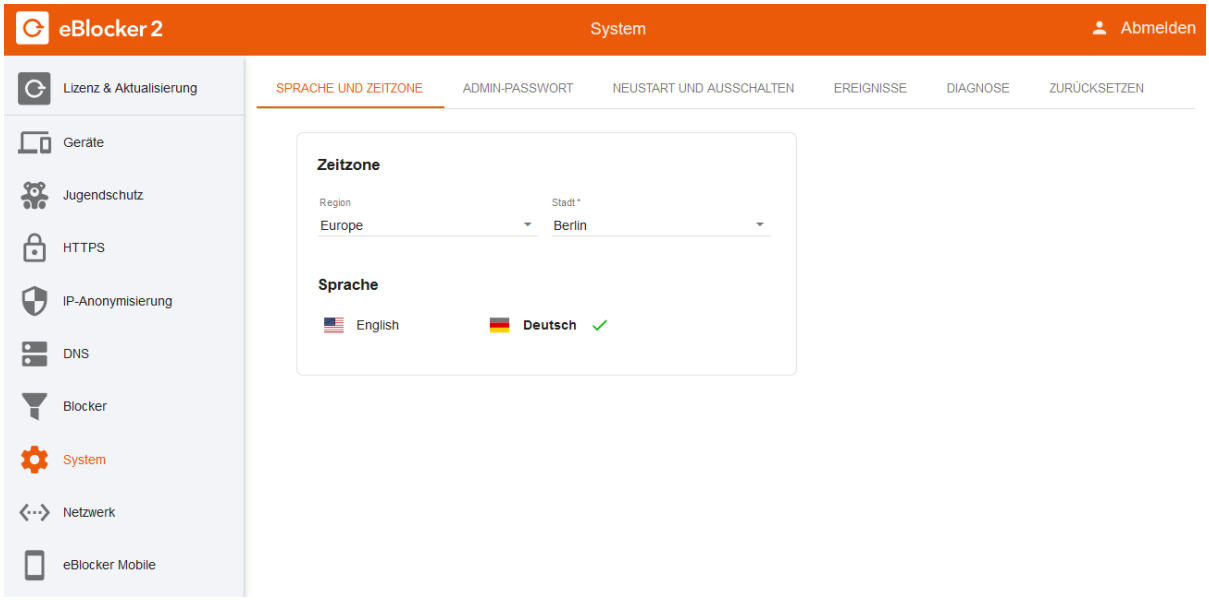
Gültig für **eBlocker Base**, **eBlocker Pro** und **eBlocker Family**

Unter „System“ können Sie folgende Einstellungen vornehmen:

8.8.1 System – Sprache und Zeitzone

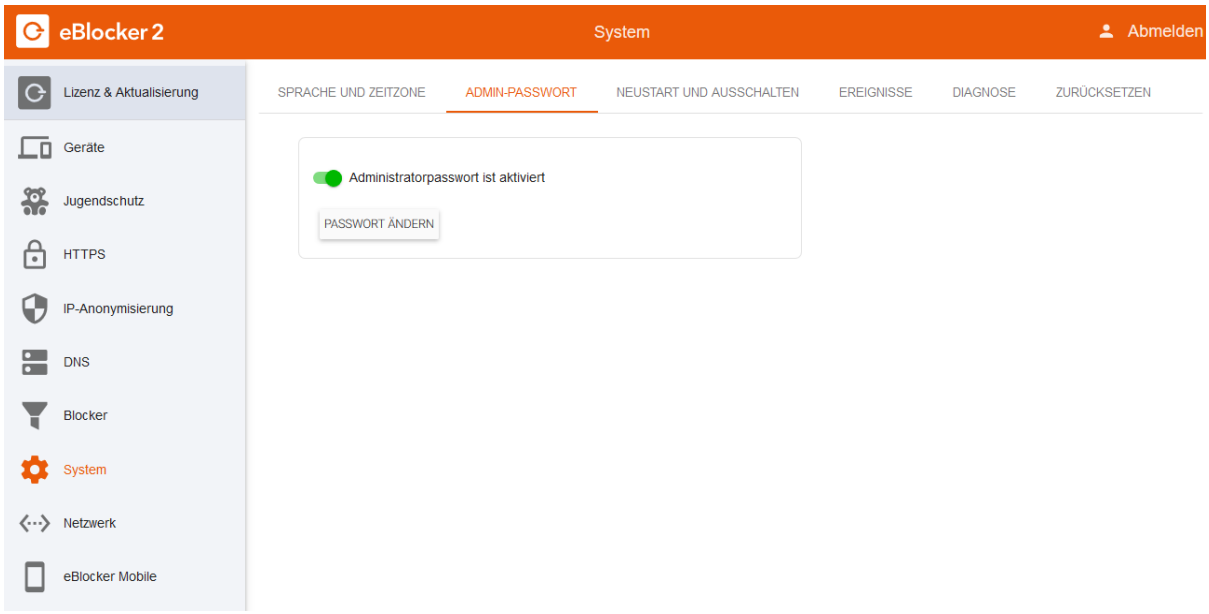
Über diese Seite können Sie die Zeitzone und die Sprache der eBlocker Controlbar und der eBlocker Konsole einstellen.Für die Einstellung der Zeitzone wählen Sie zunächst die Region und dann die Stadt Ihres Landes aus.

Für die Einstellung der Sprache, klicken Sie entweder auf Englisch oder Deutsch. Die gewünschte Sprache wird sofort umgestellt.



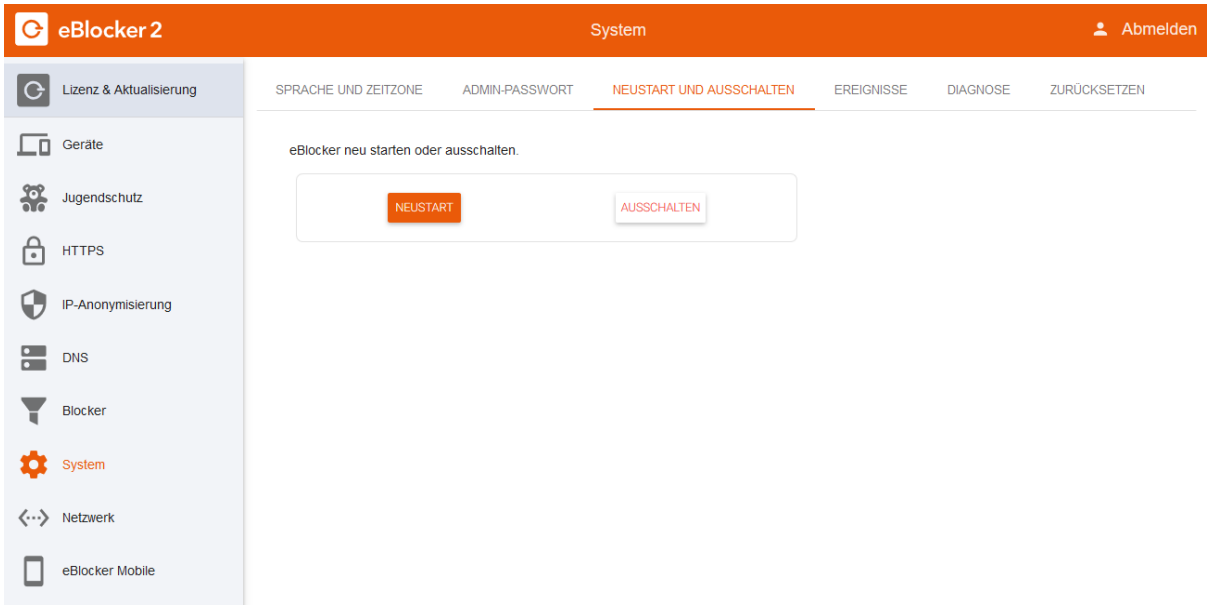
8.8.2 System - Admin-Passwort

Aktivieren Sie hier das Admin Passwort für Ihren eBlocker. Sie können auch das aktuelle Admin-Passwort ändern.



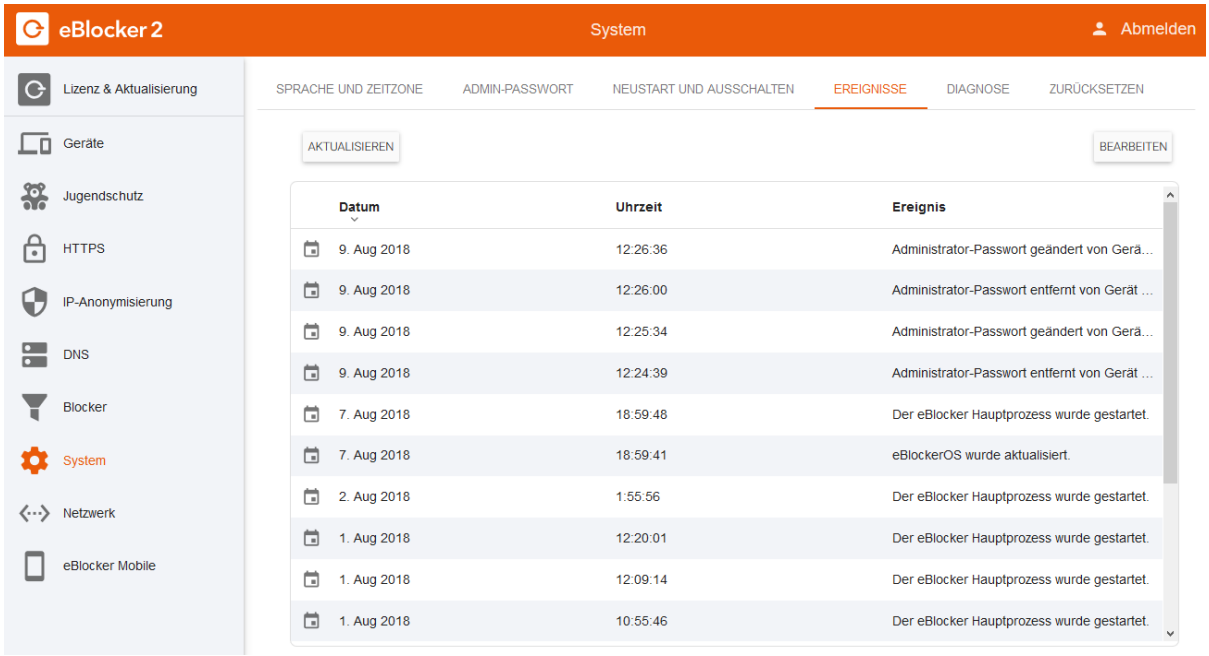
8.8.3 System - Neustarten und Ausschalten

Über diese Seite können Sie den eBlocker neu starten oder herunterfahren.
Um den eBlocker nach dem Herunterfahren erneut zu starten, ziehen Sie die Stromversorgung vom Gerät ab, warten 30 Sekunden und verbinden es anschließend wieder mit der Stromversorgung.



8.8.4 System - Ereignisse

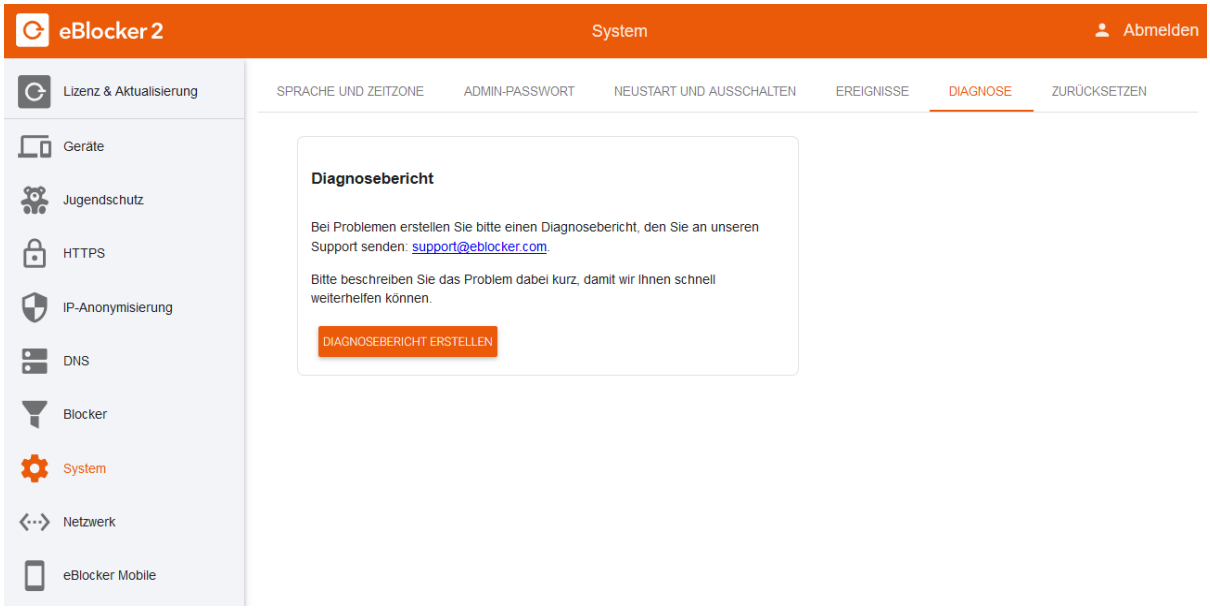
Der eBlocker erkennt Ereignisse wie etwa dass die Netzwerkverbindung getrennt, oder das Netzteil abgezogen wurde, ohne dass der eBlocker heruntergefahren wurde. Solche Ereignisse werden für Sie hier als Information festgehalten. Sie werden in der Controlbar darauf hingewiesen, wenn ein neuer Eintrag in der Ereignisliste vorliegt.



8.8.5 System - Diagnosebericht

Im Fehlerfall können Sie über diese Seite einen automatischen Diagnosebericht erstellen, den Sie an uns an die E-Mail Adresse support@eblocker.com senden können. Dies ermöglicht uns eine schnellere Lösung zu finden. Erstellen Sie den Diagnosebericht ganz einfach mit einem Klick auf den orangen

Button „Diagnosebericht erstellen“ und warten Sie einige Sekunden. Anschließend haben Sie die Möglichkeit die Datei herunterzuladen und an unseren Support zu senden. Wir melden uns schnellstmöglich bei Ihnen.



8.8.6 System – Zurücksetzen

Einstellungen Sichern

Hier haben Sie die Möglichkeit einige Ihrer Einstellungen zu sichern. So können Sie gegebenenfalls vor einem wiederherstellen der eBlocker Werkseinstellungen ein Backup anlegen und dieses nach dem wieder herstellen der Werkseinstellungen wieder einspielen.

Wenn Sie auf den Button „Einstellungen sichern“ klicken, werden folgende Daten in einer Sicherungsdatei gespeichert.

- Vertrauenswürdige Apps
- Vertrauenswürdige Websites

Die Sicherungsdatei wird in Ihrem Downloadverzeichnis gespeichert.

Um eine Sicherungsdatei wiederherzustellen reicht es, wenn Sie auf den Button „Einstellungen Wiederherstellen“ klicken und die Sicherungsdatei aus Ihrem Downloadverzeichnis auswählen.

Aktivierung zurücksetzen

Um die die Aktivierung und Lizenzbindung des Gerätes zurückzusetzen, klicken Sie auf „Aktivierung zurücksetzen“. Es erscheint ein neues Fenster, mit der Frage, ob Sie die Lizenz wirklich von dem Gerät entfernen möchten. Möchten Sie die Lizenz entfernen, geben Sie bitte die E-Mail Adresse ein, die Sie bei der Aktivierung des Gerätes verwendet haben. Bitte beachten Sie, dass dieser Vorgang nicht mehr rückgängig gemacht werden kann.

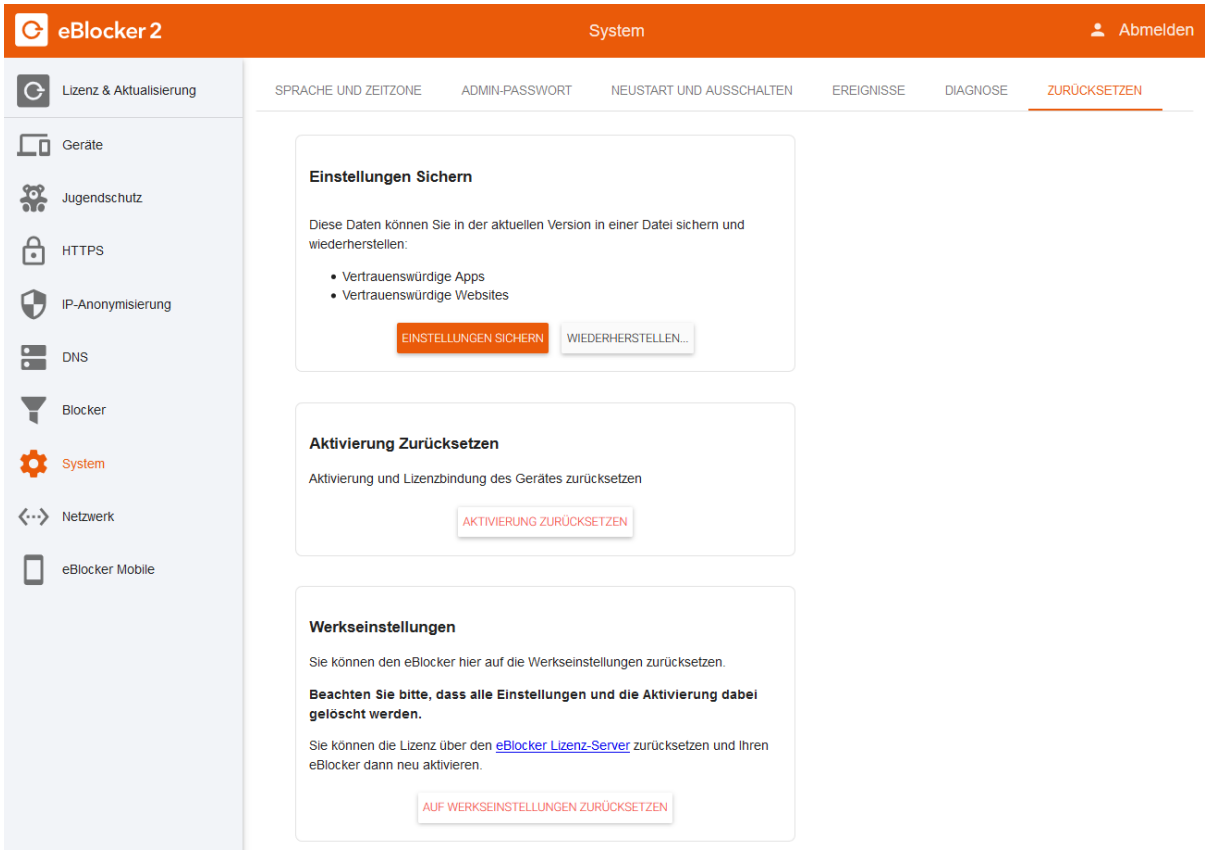
Werkseinstellungen

Hier können Sie den eBlocker auf die Werkseinstellungen zurücksetzen. Beachten Sie bitte, dass alle Einstellungen und die Aktivierung dabei gelöscht werden.

Sie können die Lizenz über den eBlocker Lizenz-Server zurücksetzen und Ihren eBlocker dann neu aktivieren. Gehen Sie dazu bitte auf die Website https://www.eblocker.com/de/lizenztransfer/ und geben Sie dort die Mailadresse ein, mit welcher Sie die eBlocker Lizenz aktiviert haben. Im Anschluss

erhalten Sie eine Mail von unserem Lizenz-Server und brauchen nur den Anweisungen dieser Mail folgen.Hier können Sie den eBlocker auf die Werkseinstellungen zurücksetzen. Beachten Sie bitte, dass alle Einstellungen und die Aktivierung dabei gelöscht werden.

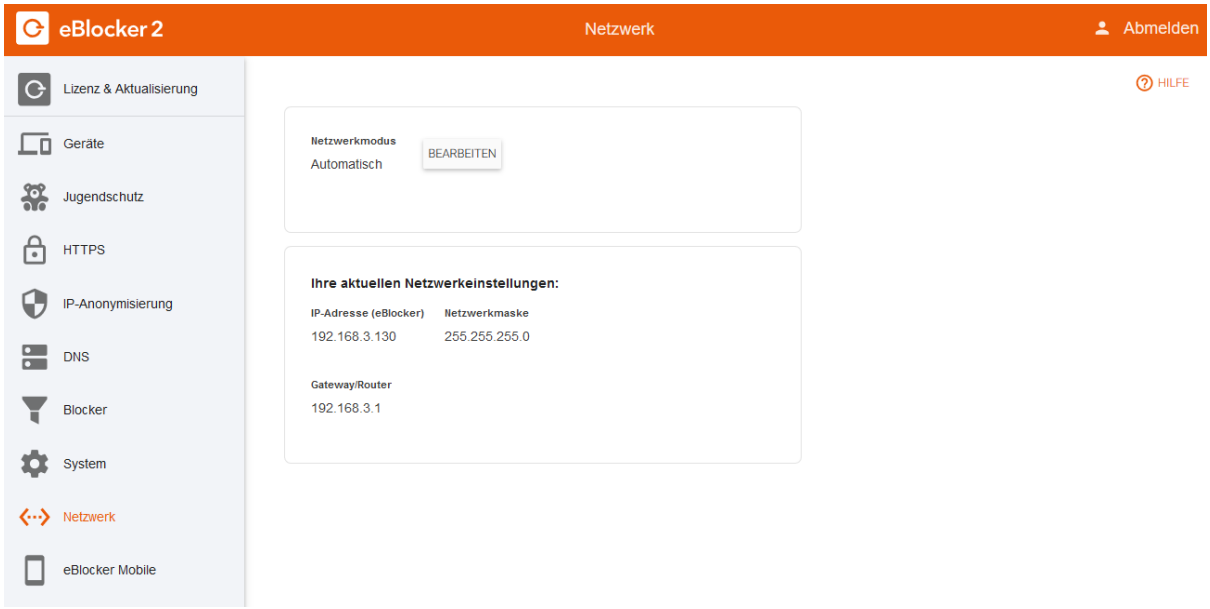
Sie können die Lizenz über den eBlocker Lizenz-Server zurücksetzen und Ihren eBlocker dann neu aktivieren. Gehen Sie dazu bitte auf die Website https://www.eblocker.com/de/lizenztransfer/ und geben Sie dort die Mailadresse ein, mit welcher Sie die eBlocker Lizenz aktiviert haben. Im Anschluss erhalten Sie eine Mail von unserem Lizenz-Server und brauchen nur den Anweisungen dieser Mail folgen.



8.9 Netzwerk

Gültig für **eBlocker Base**, **eBlocker Pro** und **eBlocker Family**

In den meisten Fällen kann der eBlocker im automatischen Konfigurationsmodus betrieben werden.



In manchen Fällen, zum Beispiel wenn Sie eine besondere Netzwerkinfrastruktur haben, kann es nötig sein, die Netzwerkkonfiguration des eBlockers umzustellen, um den eBlocker optimal nutzen zu können.

Der eBlocker bietet drei verschiedene Netzwerkmoduse an:

Automatischer Netzwerkmodus

In diesem Modus vergibt Ihr Router mit seinem DHCP-Dienst die IP-Adressen in Ihrem Netzwerk. Der eBlocker ist mit den meisten Router kompatibel, aber es gibt einige wenige Router, die so nicht mit dem eBlocker zusammen arbeiten.

Individuelle Einstellungen

In diesem Modus vergibt der eBlocker die IP-Adressen im Netzwerk. Dazu muss der DHCP-Dienst des Routers abgeschaltet werden. Der eBlocker übernimmt dann die Aufgaben des DHCP-Diensts in Ihrem Netzwerk. So gut wie alle Router sind in diesem Modus kompatibel mit dem eBlocker. Sie werden durch

die Einrichtung der „individuellen Einstellungen“ von einem Assistenten begleitet, welcher Ihnen Schritt für Schritt Hilfestellungen gibt.

Expertenmodus

In diesem Modus können erfahrene Benutzer die Netzwerkeinstellungen des eBlockers bearbeiten. Diese Einstellungen machen Sinn, wenn Sie zum Beispiel einen eigenen DHCP-Server in Ihrem Netzwerk betreiben.

8.9.1 eBlocker Mobile

eBlocker Mobile basiert im Kern auf OpenVPN. Ihr eBlocker wird damit zum VPN-Server, zu dem Sie sich von einem mobilen Gerät verbinden können. Sobald Sie mit dem eBlocker per OpenVPN verbunden sind, surfen Sie unterwegs mit genau demselben Schutz, den Sie von zu Hause gewohnt sind. Dazu ist die Installation eines OpenVPN Clients für Ihr mobiles Gerät sowie die Installation der entsprechenden eBlocker VPN-Konfigurationsdatei notwendig.

Sie benötigen eine der folgenden kostenlosen Apps für Ihr Betriebssystem, um einen VPN-Tunnel zu Ihrem Heimnetzwerk zu öffnen:

OpenVPN App für macOS

Tunnelblick (Open Source GNU General Public License)

Tunnelblick
OpenVPN for Mac OS X

OpenVPN App für iOS

OpenVPN Connect for iPhone

Download on the App Store

OpenVPN Connect for iPad

Download on the App Store

OpenVPN App für Android

OpenVPN Connect

GET IT ON Google Play

Nachdem Sie erfolgreich eine OpenVPN App für Ihr Betriebssystem installiert haben, muss nun die eBlocker Mobile Konfigurationsdatei geladen und in der OpenVPN App hinzugefügt werden.

Alle Schritte müssen auf genau dem Gerät ausgeführt werden, von dem aus Sie von unterwegs den Schutz Ihres eBlocker nutzen möchten! Sie müssen während der Installation mit Ihrem Heimnetzwerk verbunden sein.

Android

- Laden Sie die OpenVPN Konfigurationsdatei für dieses Gerät.
- Bestätigen Sie „In OpenVPN öffnen“.
- Es öffnent sich automatisch die OpenVPN App.
- Bestätigen Sie den Import der Datei mit einem Tap auf das grüne „+“
- Bewegen Sie den Schieberegler nach rechts um die Verbindung zu starten.
- Nach erfolgreichem Verbindungsaufbau erscheint das VPN Symbol am oberen Bildschirmrand & und innerhalb der App läuft ein Zähler.
- Nach einem Neustart Ihres Smartphones müssen Sie den Schieberegler erneut betätigen.

iOS

- Laden Sie die OpenVPN Konfigurationsdatei für dieses Gerät.
- Bestätigen Sie „DATEI ÖFFNEN“ am unteren Bildrand.
- Es öffnet sich automatisch die OpenVPN App.
- Bestätigen Sie den Import der Datei mit „Ok“.
- Sie befinden sich jetzt in der App „OpenVPN“, bewegen Sie den Schieberegler nach rechts um die Verbindung zu starten.
- Ein grüner Schieberegler signalisiert den erfolgreichem Verbindungsaufbau, ausserdem erscheint ein kleines grünes Icon am oberen Bildschirmrand.
- Nach einem Neustart Ihres Smartphones müssen Sie den Schieberegler erneut betätigen.

WINDOWS

- Gehen Sie mit dem Windows Gerät mit welchem sie eBlocker mobile Nutzen möchten, ins eBlocker Dashboard
- Laden Sie auf der Karte eBlocker Mobile die OpenVPN Konfigurationsdatei herunter.
- Lokalisieren Sie die heruntergeladene OpenVPN Konfigurationsdatei im Ordner für heruntergeladene Dateien (Name der Datei: eBlocker_Mobile_MyEBlockerovpn)
- Kopieren Sie die OpenVPN Datei in den Ordner für Konfigurationsdateien. Dies ist in der Regel c:\tbd
- Starten Sie die OpenVPN App. Häufig ist diese schon gestartet.
- Wählen Sie in der Taskleiste das OpenVPN-Symbol und dort die eBlocker Konfiguration
- Ihr Computer verbindet sich mit Ihrem eBlocker ein.
- Nach einem Neustart oder Netzwerkausfall starten Sie die Verbindung einfach wieder in der Taskleiste.

macOS

- Laden Sie die OpenVPN Konfigurationsdatei für dieses Gerät.
- Lokalisieren Sie das heruntergeladene OpenVPN Konfigurationsdatei im Ordner für heruntergeladene Dateien (Name der Datei: eBlocker_Mobile_MyEBlockerovpn)
- Doppelklicken Sie die geladene .ovpn-Datei
- Bestätigen Sie den Installationsdialog
- Klicken Sie auf das Tunnelblick Icon in der Menüleiste
- Wählen Sie „eBlocker_Mobile_MyEBlocker verbinden“
- Ihr Mac verbindet sich jetzt mit Ihrem eBlocker.
- Nach einem Neustart oder Netzwerkausfall starten Sie die Verbindung einfach wieder mit dem Icon in der Menuleiste.

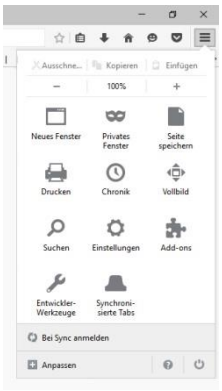
9 Kurzanleitungen

9.1 Cookies, Cache und Browserhistorie im Browser löschen

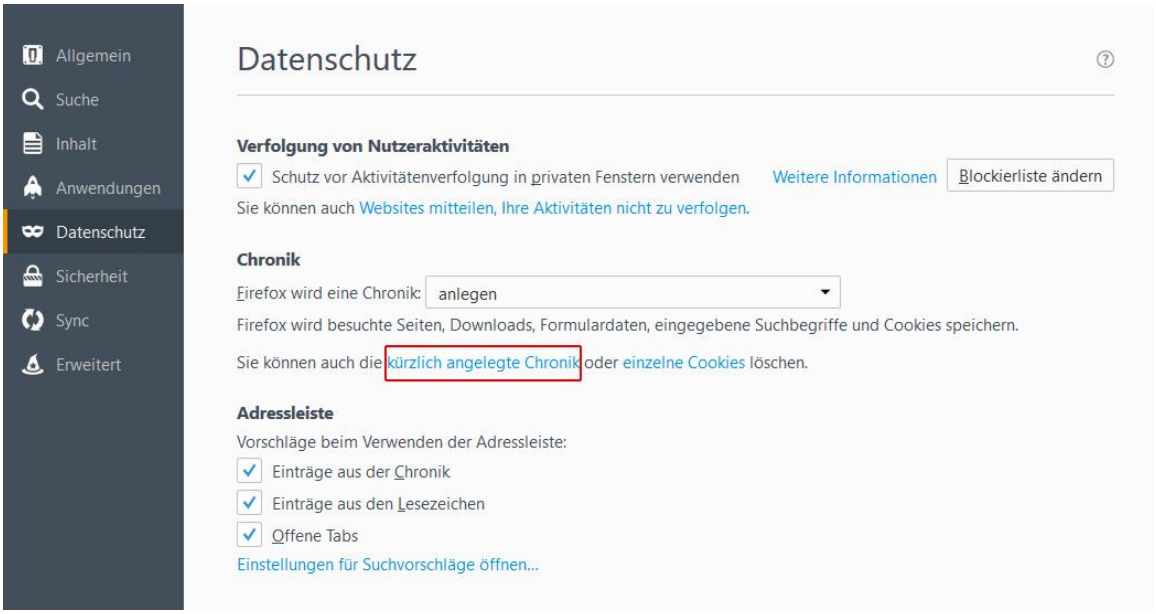
Abhängig vom verwendeten Browser ist das Vorgehen zum Löschen von Cookies unterschiedlich. Nachfolgend wird der Vorgang für die wichtigsten Browser beschrieben. Wenn Ihr Browser hier nicht aufgeführt ist, folgende Sie bitte der Anleitung Ihres Browsers zum Löschen von Cookies, Cache und Browser Historie.

9.1.1 Firefox

Öffnen Sie Ihren Browser und klicken Sie auf das Menü Symbol oben rechts im Browser. Es erscheint ein Fenster mit verschiedenen Optionen.



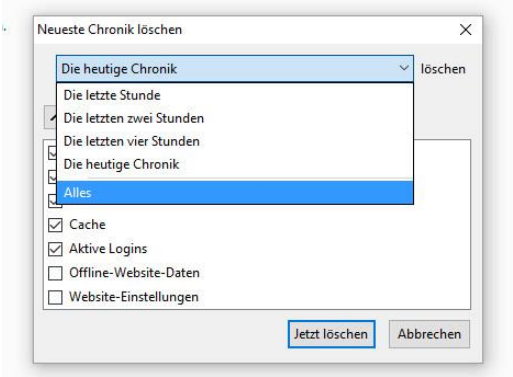
Klicken Sie auf „Einstellungen“ und gehen Sie anschließend auf „Datenschutz“.



Klicken Sie auf „kürzlich angelegte Chronik“. Es erscheint ein neues Fenster, in das Sie überall für Sie relevante Themen, Häkchen einfügen können. Wir empfehlen Ihnen folgende Optionen anzukreuzen, um Ihre Spur nach dem Browsen vollständig zu löschen:

- Besuchte Seiten & Download-Chronik
- Cookies
- Eingegebene Suchbegriffe & Formulardaten
- Offline-Website-Daten

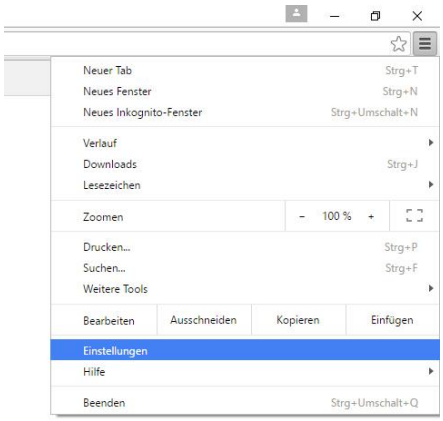
Unter „Die heutige Chronik“ haben Sie die Möglichkeit den Zeitraum festzulegen. Wir empfehlen auch hier „Alles“ auszuwählen, um einen umfassenden Schutz vor Spionage zu erhalten.



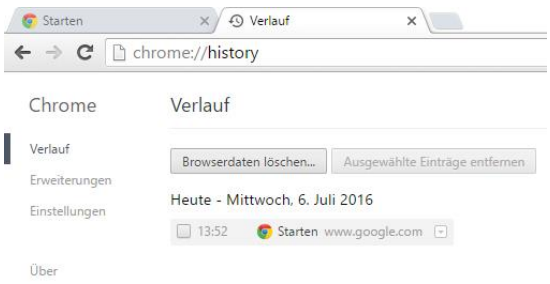
Beenden Sie den Vorgang anschließend mit „Jetzt löschen“.

9.1.2 Chrome

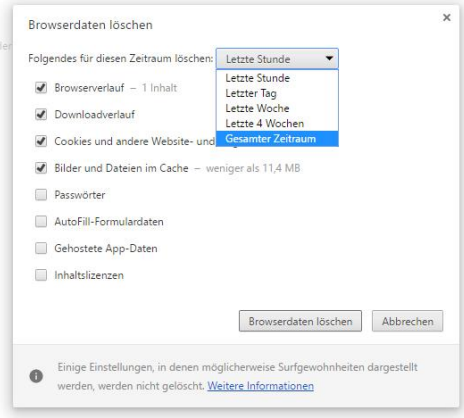
Öffnen Sie Ihren Browser und klicken Sie auf das Menü Symbol oben rechts im Browserfenster.



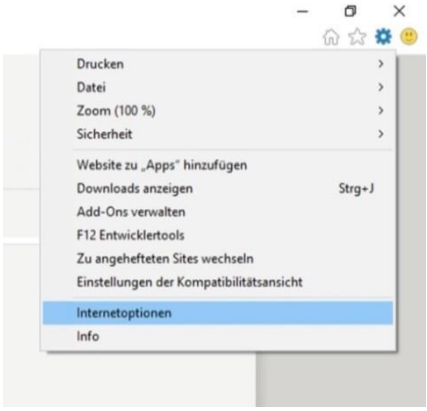
Gehen Sie auf „Einstellungen“ und klicken Sie auf „Verlauf“. Beenden Sie den Vorgang mit „Browserdaten löschen“.



Bitte beachten Sie, dass auch hier der „gesamte Zeitraum“ angegeben ist.

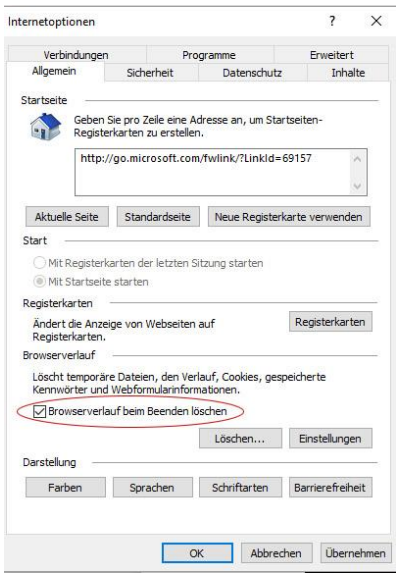


9.1.3 Internet Explorer



Klicken Sie auf das Zahnrad Symbol oben rechts im Browserfenster. Gehen Sie auf „Internetoptionen“ und anschließend auf „Allgemein“.

Beenden Sie den Vorgang mit „Browserverlauf löschen“.



10 Glossar

- **Content Sperre**

Anbieter von (z.B.) journalistischen Inhalten haben ein legitimes Recht – und natürlich auch die Notwendigkeit – mit ihrem Angebot Geld zu verdienen. Bei vielen Anbietern hat der Leser die Wahl, den Inhalt entweder direkt einzeln oder per Abo zu bezahlen – oder eben zu akzeptieren, dass die aufgerufene Webseite Werbung enthält.

Manche Anbieter behalten sich das Recht vor, den kostenlosen Dienst zu sperren, wenn der Nutzer einen Ad-Blocker verwendet. Diese Sperre nennt man auch „Content Sperre“.

eBlocker hat nicht das Ziel, das Geschäftsmodel von Anbietern im Internet zu zerstören. Wir blockieren allerdings auch die Werbung aus Werbenetzwerken auf solchermaßen finanzierten Seiten, weil die Werbebanner heutzutage immer auch zur Profilbildung verwendet werden.

Wir helfen aber nicht dabei, die angegebenen Content Sperren zu umgehen. Stattdessen empfehlen wir, qualitativ hochwertigen Inhalt auf anderem Wege fair zu honorieren. Damit uns allen unabhängiger Qualitätsjournalismus dauerhaft erhalten bleibt.

- **Cookies**

Cookies enthalten typischerweise Daten über besuchte Webseiten, die der Webbrowser beim Besuch dieser Webseiten auf Ihrem Computer speichert und beim nächsten Besuch der gleichen Website wieder verwenden kann.

Cookies sind nicht grundsätzlich schlecht. Viele moderne Webanwendungen würden ohne Cookies gar nicht funktionieren. Sie können den Bedienungskomfort erhöhen, z.B. wenn man sich beim erneuten Besuch einer Website nicht neu anmelden muss.

Cookies können aber auch dafür verwendet werden, um Sie auf verschiedenen Websites immer wieder als das gleiche Individuum erkennen zu können und um umfassende Profildaten von Ihnen zu sammeln und zu verdichten. Diese Tracking-Cookies werden vom eBlocker blockiert, so dass sie gar nicht erst auf Ihrem Computer angelegt werden.

- **DHCP Server und DHCP Lease**

Das Dynamic Host Configuration Protocol (DHCP) ermöglicht die automatische Integration von Netzwerkgeräten in ein Netzwerk. Dabei weist ein zentraler Server – meist der Router – allen anderen Geräten ihre Netzwerkkonfiguration zu. Die Lebensdauer so einer Zuweisung nennt man Lease-Time. Am Router kann der Administrator bestimmen, wie lange diese Lease-Time Bestand hat. Die Lease-Time kann meist in Sekunden, Tage oder sogar Wochen angegeben werden.

Wird jetzt im laufenden Betrieb der DHCP Server gewechselt, muss bei allen Rechnern / Endgeräten die Verbindung zum Netzwerk einmal kurz getrennt werden, damit sich jedes Gerät bei dem neuen DHCP Server meldet und einen DHCP Lease erhält.

- **Digitales Zertifikat**

Ein digitales Zertifikat verwendet kryptografische Methoden, um Angaben zu einem Kommunikationspartner verbindlich und überprüfbar zu bestätigen. Zum Beispiel, dass eine bestimmte Website tatsächlich von der angegebenen Firma betrieben wird. Digitale Zertifikate werden üblicherweise von vertrauenswürdigen Zertifizierungsstellen ausgestellt, die die Angaben geprüft haben und für die Korrektheit einstehen.

- **DNS-Server**

Der DNS-Server (Domain Name System) ist eine Art Telefonbuch für das Internet. Es übersetzt die Servernamen aus URLs und aus E-Mail-Adressen in nummerische IP-Adressen. Über die IP-Adresse wird dann der Webserver identifiziert und angesprochen.

- **LAN-Kabel**

Das LAN-Kabel (Local Area Network) oder auch Ethernet-Kabel ist ein Netzwerkkabel für den Anschluss von Computern und anderen Netzwerkgeräten an das lokale Netz. Ethernet-Kabel sind oft gelb. Das beim eBlocker mitgelieferte LAN-Kabel ist natürlich orange!

- **Netzwerkmaske**

Die Netzwerkmaske legt in Verbindung mit der IP-Adresse eines Rechners fest, welche anderen IP-Adressen zum lokalen Netz gehören. D.h. welche Adressen direkt und ohne Umweg erreicht werden können. Alle anderen IP-Adressen, die nicht unter die gleiche Netzwerkmaske fallen, gehören nicht zum lokalen Netz und können nur über den Router erreicht werden.

- **Preisdiskriminierung**

Preisdiskriminierung bezeichnet eine Preispolitik im Internet, bei der für die gleiche Leistung je nachdem wer die Anfrage stellt, ein höherer oder ein geringerer Preis aufgerufen wird. Hierbei wird der Preis anhand der über den Nutzer bekannten Daten dynamisch festgelegt, mit dem Ziel den Umsatz zu maximieren.

- **Referrer**

Wenn Sie eine Webseite in Ihrem Browser aufrufen, schickt der Browser eine entsprechende Anfrage an den angesprochenen Webserver. Diese Anfrage enthält nicht nur die URL, sondern zahlreiche weitere Meta-Daten zur Anfrage. Unter anderem übermittelt der Browser, von welcher Webseite aus die neue Anfrage gestartet wurde.

Diese Angabe wird gemeinhin als „HTTP-Referrer“ oder kurz als „Referrer“ bezeichnet.

Sie hat den legitimen Zweck, innerhalb einer Website verfolgen zu können, welche Seiten ein Nutzer in Folge aufruft und das Angebot entsprechend zu optimieren. Sie kann aber auch Website-übergreifend verwendet werden, um Benutzerprofile zu erstellen und zu verknüpfen.

- **Schadsoftware**

Schadsoftware ist der Oberbegriff für gefährliche Computerprogramme wie z.B. Viren, Würmer oder Trojaner. Schadsoftware kann beim Besuch von infizierten Websites oder durch Öffnen von infizierten E-Mails auf Ihren Computer gelangen. Auch Werbebanner, die auf eigentlich vertrauenswürdigen Websites eingeblendet werden, können Schadsoftware enthalten.

Nicht jede Schadsoftware macht sich sofort (oder überhaupt) bemerkbar.

Der beste Schutz vor Schadsoftware ist es, das System immer so aktuell wie möglich zu halten; keine verdächtigen E-Mails zu öffnen; nicht auf Links aus zweifelhafter Quelle zu klicken; ein aktuelles Antiviren-Programm zu verwenden. Und natürlich den eBlocker einzusetzen.

- **SSL Verschlüsselung**

Die SSL (Secure Sockets Layer) Verschlüsselung ist ein Verfahren zur Datenverschlüsselung. Sie sorgt in Verbindung mit den Zertifikaten dafür, dass auf dem Weg vom Server zu einem Browser keine Änderungen an den Daten vorgenommen werden können und dass die ausgetauschten Daten nicht von unberechtigten Personen gelesen werden.
Meldet sich ein Internetnutzer zum Beispiel bei einem Forum oder einem Online Shop an, können dessen Anmeldedaten und Texte bei Versand ohne SSL Verschlüsselung leicht eingesehen und später missbraucht werden. Wird die Verbindung mittels SSL Verschlüsselung geschützt, bedeutet es einen relativ hohen Aufwand diese Verschlüsselung auszuhebeln.

- **Tor-Netzwerk**

Das Tor-Netzwerk dient dazu, die ursprüngliche IP-Adresse zu verschleiern und eine anonyme Internetnutzung zu ermöglichen. Angenommen Sie möchten eine Seite besuchen und geben die URL in den Webbrowser ein. Ihre IP-Adresse wird direkt an die Seite geschickt, die Sie besuchen möchten. Benutzen Sie aber Tor, landen Sie im Tor-Netzwerk, welches aus vielen weiteren IP-Adressen von

verschiedenen Rechnern besteht. Aus dem Tor-Netzwerk heraus wird dann aus Zufall eine beliebige IP-Adresse an die Seite gesendet die Sie besuchen möchten. Somit bleibt Ihre wirkliche IP-Adresse verschleiert.

- **Tracker - Datensammler**

Tracker sind oft Dienstleister für die Werbeindustrie. Sie bezahlen Webseitenbetreiber dafür, dass diese unsichtbare Tracking-Aufrufe auf ihre Webseiten stellen. Jedes Mal, wenn jemand eine dieser Seiten aufruft, bekommt auch der Tracker eine entsprechende Nachricht übermittelt. Über entsprechende Cookies oder andere Verfahren kann der Tracker den Internet-Nutzer über unterschiedliche Webseiten hinweg immer wieder erkennen und so ein detailliertes Protokoll seines Internet-Verhaltens erstellen.

Die Tracker selbst verdienen ihr Geld in der Regel damit, dass sie diese Persönlichkeitsprofile wiederum der Werbeindustrie zur Verfügung stellen. Die kann nun zielgerichtet und genau auf Ihre Interessen zugeschnittene Werbung auf den Seiten platzieren, die Sie in Zukunft besuchen.

- **openVPN**

OpenVPN ist eine freie Software zum Aufbau eines Virtuellen Privaten Netzwerkes (VPN) über eine verschlüsselte Verbindung.

- **VPN**

Ein Virtuelles Privates Netzwerk (VPN) erweitert ein privates Netzwerk über ein öffentliches Netzwerk und ermöglicht es Benutzern, Daten über das öffentliche Netze zu senden und zu empfangen, als ob ihre Computergeräte direkt mit dem privaten Netzwerk verbunden wären.

Anhang A Technische Spezifikationen (nicht gültig für Software Lizenzen)

- 1 x 10/100/1000 LAN RJ45
- 1 x Stromversorgung 5V (≥ 2A)
- 1 x Wifi 802.11 b/g/n
- 2 x USB 2.0 (für Erweiterungen)
- 1 x HDMI (ohne Funktion)
- Energieverbrauch: <10W
- Abmessungen: 9x9x9cm
- Gewicht: ca. 153g

Anhang B Sicherheitshinweise

Beachten Sie vor dem Anschluss Ihres eBlocker die folgenden Sicherheitshinweise, um den eBlocker vor Schäden zu bewahren.

- Der eBlocker hat keinen Ein- oder Ausschalter. Eine Trennung des eBlockers vom Stromnetz sollte jederzeit möglich sein.
- Stellen Sie vor der Wandmontage des eBlockers sicher, dass sich hinter den geplanten Bohrstellen keine Leitungen befinden.
- Schützen Sie den eBlocker vor Nässe, Staub, Flüssigkeiten und Dämpfen.
- Verdecken Sie nicht die Lüftungsschlitze des eBlockers.
- Unterbrechen Sie niemals die Stromzufuhr oder Netzwerkverbindung während eines Updates. Dies kann den eBlocker irreparabel beschädigen.

Anhang C Herstellerinformation

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

Anhang D Technischer Support

Web: http://forum.eBlocker.com
E-Mail: support@eBlocker.com

Einen telefonischen Support bieten wir leider derzeit nicht an.

Anhang E CE-Konformitätserklärung

Hiermit erklärt eBlocker, dass das Gerät eBlocker Pro, eBlocker Family den Richtlinien 2014/53/EU sowie 2011/65/EU entspricht.

Der vollständige Text der EU-Konformitätserklärung ist unter der folgenden Internetadresse in englischer Sprache abrufbar: https://www.eblocker.com/de/konformitaetserklaerungen/

Anhang F Entsorgung von Altgeräten

Das Symbol des durchgestrichenen Mülleimers besagt, dass dieses Elektro- bzw. Elektronikgerät am Ende seiner Lebensdauer nicht im Hausmüll entsorgt werden darf. Zur Rückgabe stehen in Ihrer Nähe kostenfreie Sammelstellen für Elektro- und Elektronikaltgeräte zur Verfügung. Die Adressen erhalten Sie von Ihrer Stadt- bzw. Kommunalverwaltung. Durch die separate Sammlung von Elektro- und Elektronikaltgeräten soll die Wiederverwendung, die stoffliche Verwertung bzw. andere Formen der Verwertung von Altgeräten ermöglicht sowie negative Folgen bei der Entsorgung der in den Geräten möglicherweise enthaltenen gefährlichen Stoffe auf die Umwelt und die menschliche Gesundheit vermieden werden. Weitere Informationen finden Sie auf www.elektrogesetz.de.

Firmware-Version
eBlocker Base/Pro/Family 2.0 20180830-v57