Firefox/Privacy

< Firefox

This article overviews how to configure **Firefox** to enhance security and privacy.

Contents

Related articles

Firefox

Tor

Browser Plugins

Firefox/Tweaks

Firefox/Profile on RAM

Configuration tweaks

The following are privacy-focused configuration tweaks to prevent **browser fingerprinting (https://panopticlick.eff.org/)** and tracking.

In addition, see the following links:

- **How to stop Firefox from making automatic connections (https://support.mozilla.org/t5/Protect-your-privacy/How-to-stop-Firefox-from-making-automatic-connections/ta-p/1748)** - Is an annotated list of corresponding Firefox functionality and settings to disable it case-by-case.
- **ffprofile.com (https://ffprofile.com/)** - You select which features you want to enable and disable and in the end you get a download link for a zip-file with your profile template. You can for example disable some functions, which send data to Mozilla and Google, or disable several annoying Firefox functions like Mozilla Hello or the Pocket integration.
- **pyllyukko/user.js (https://github.com/pyllyukko/user.js)** - Firefox configuration hardening and documentation

Enable Anti-Fingerprinting

Mozilla has started an **anti-fingerprinting project in Firefox (https://wiki.mozilla.org/Security/Fingerprinting)**, as part of a project to upstream features from **Tor Browser**. Many of these anti-fingerprinting features are enabled by setting `about:config`:

- `privacy.resistFingerprinting` `true`

There is no user-facing documentation about this flag, and Mozilla doesn't recommend users enable it, since it will break a few websites (it exists mostly to make life easier for the Tor Browser developers). But it does automatically enable many of the features listed below (such as changing your reported timezone and user agent), as well as protection against other, lesser-known fingerprinting techniques. See the **tracking bug (https://bugzilla.mozilla.org/show_bug.cgi?id=1333933)** that lists many of these features.

Enable tracking protection

Firefox gained an option for **tracking protection (https://support.mozilla.org/en-US/kb/tracking-protection-firefox)**. It can be enabled by setting `about:config`:

- `privacy.trackingprotection.enabled` `true`

Apart from privacy benefits, enabling **tracking protection (http://venturebeat.com/2015/05/24/firefoxs-optional-tracking-protection-reduces-load-time-for-top-news-sites-by-44/)** may also reduce load time by 44%.

Note that this is not a replacement for ad blocking extensions such as **#uBlock Origin** and it may or may not work with **Firefox forks**.

Change browser time zone

The time zone of your system can be used in browser fingerprinting. To set firefox's time zone to UTC launch it as:

```
$ TZ=UTC firefox
```

Or, set a script to launch the above (for example, at `/usr/local/bin/firefox`).

Change user agent and platform

You can override Firefox's user agent with the `general.useragent.override` preference in `about:config`.

The value for the key is your browser's user agent. Select a known common one.

Tip: The value `Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52.0` is used as the user agent for the Tor browser, thus being very common.

Warning: Changing the user agent without changing to a corresponding platform will make your browser nearly unique.

To change the platform for firefox, add the following `string` key in `about:config`:

```
general.platform.override
```

Select a known common platform that corresponds with your user agent.

Tip: The value `Win32` is used as the platform for the Tor browser, corresponding with the user agent provided above.

WebRTC exposes LAN IP address

To prevent websites from getting your local IP address via **WebRTC**'s peer-to-peer (and JavaScript), open `about:config` and set:

- `media.peerconnection.ice.default_address_only` to `true`
- `media.peerconnection.enabled` to `false`. (only if you want to completely disable WebRTC)

You can use this **WebRTC test page (http://net.ipcalf.com/)** and **WebRTC IP Leak VPN / Tor IP Test (https://www.privacytools.io/webrtc.html)** to confirm that your internal/external IP address is no longer leaked.

Disable 1024-bit Diffie-Hellman primes

Following **recent research (https://freedom-to-tinker.com/blog/haldermanheninger/how-is-nsa-breaking-so-much-crypto/)** it is likely that the NSA has been breaking 1024-bit Diffie-Hellman for some time now. To disable these switch the **following (https://www.eff.or**

g/deeplinks/2015/10/how-to-protect-yourself-from-nsa-attacks-1024-bit-DH) settings to `false` in `about:config`:

```
security.ssl3.dhe_rsa_aes_128_sha
security.ssl3.dhe_rsa_aes_256_sha
```

Then consider checking your SSL configuration at https://www.howsmyssl.com/.

Disable telemetry

Set `toolkit.telemetry.enabled` to `false` and/or disable it under Preferences, Advanced, Data Choices.

Enable Do Not Track Header (DNT)

Note: The remote server may choose to not honour the Do Not Track request.

Set `privacy.donottrackheader.enabled` to `true` or toggle it in *Preferences* > *Privacy* > *Manage your Do Not Track settings*.

Disable geolocation

Set `geo.enabled` to `false` in `about:config`.

Disable Safe Browsing service

Safe Browsing offers phishing protection and malware checks, however it may send user information (e.g. URL, file hashes, etc.) to third parties like Google.

To disable the Safe Browsing service, in `about:config` set:

- `browser.safebrowsing.malware.enabled` to `false`
- `browser.safebrowsing.phishing.enabled` to `false`

In addition disable download checking, by setting `browser.safebrowsing.downloads.enabled` to `false`.

Disable WebGL

WebGL is a potential security risk.**[1] (http://security.stackexchange.com/questions/13799/is-webgl-a-security-concern)** Set `webgl.disabled` to `true` in `about:config` if you want to disable it.

Extensions

HTTPS Everywhere

HTTPS Everywhere (https://www.eff.org/https-everywhere) is an extension which encrypts your communication with a website. It forces a connection over HTTPS instead of HTTP wherever possible.

HTTPS Everywhere will be automatically configured and enabled upon restarting Firefox. For information on how to set up your own rules for different websites please visit **the official website (https://www.eff.org/https-everywhere/rulesets)**.

Note: HTTPS Everywhere does not magically enable HTTPS for every site on the internet. The site needs to support HTTPS and HTTPS Everywhere should have a ruleset configured for that site.

uBlock Origin

uBlock Origin is a lightweight, efficient blocker which is easy on **memory and CPU (https://github.com/gorhill/uBlock#performance)**. It comes with several filter lists ready to use out-of-the-box (including EasyList, Peter Lowe's, several malware filter lists).

The lead developer of uBlock forked the project and created uBlock Origin. As of July 2015, most of the development is being done on uBlock Origin and the codebases are deviating substantially.

uBlock Origin: **Github (https://github.com/gorhill/uBlock)**; **Firefox Add-ons (https://addons.mozilla.org/firefox/addon/ublock-origin/)**.

AdNauseam

AdNauseam (https://adnauseam.io/) is a lightweight browser extension that blends software tool and artware intervention to fight back against tracking by advertising networks. AdNauseam works like an ad-blocker (it is built atop uBlock-Origin) to silently simulate clicks on each blocked ad, confusing trackers as to one's real interests **[2] (https://github.com/dhowe/AdNauseam/)**.

Adblock Plus

Adblock Plus (https://adblockplus.org/en/) was a popular extension to block ads. Now that it is not blocking some ads on purpose **[3] (https://adblockplus.org/acceptable-ads)**, it may be a better idea to use a different blocker like uBlock Origin.

Privacy Badger

Privacy Badger (https://www.eff.org/privacybadger) is an extension that monitors third-party trackers loaded with web content. It blocks trackers once they appear on different sites. It does not block advertisements in the first place, but since a lot of ads are served based on tracking information these are blocked as well. For more information on the mechanism, see its **FAQ (https://www.eff.org/privacybadger#faq-How-is-Privacy-Badger-different-to-Disconnect,-Adblock-Plus,-Ghostery,-and-other-blocking-extensions?)**.

Disconnect

Disconnect is a open source project aimed at stopping 2,000 third-party sites from tracking a user. It encrypts data sent to popular sites and claims to loads web pages 27 percent faster. Disconnect shows its users, in real time, how many tracking attempts from Google, Twitter, Facebook, and more are stopped. It categorizes tracking attempts into advertising, analytical, social, and content, which makes it easy to monitor how one is being tracked.

Disconnect can also stop side-jacking, which utilizes stolen cookies to steal personal data. It is easy to use and well supported. It can be added to Firefox at the **official website (https://disconnect.me/)**.

> **Note:** Firefox gained a feature based on the Disconnect list. See **#Enable tracking protection**.

NoScript

NoScript (http://noscript.net/) is an extension which disables JavaScript, Java, Flash and other plugins on any website not specifically whitelisted by the user. This extension will protect you from exploitation of security vulnerabilities by not letting anything but trusted sites (e.g: your bank, webmail) serve you executable content.

Once installed you can configure settings for NoScript by either clicking its icon on the toolbar or right clicking a page and navigating to NoScript. You will then have the option to enable/disable scripts for the current page, as well as any third party scripts that the page is linking to. Alternatively you can choose to enable scripts temporarily for that session only.

Be aware a lot of modern websites use scripts for layout purposes, hence content may look different. For example, failed rendering due to missing fonts might occur on websites that load fonts at runtime via scripts, which were blocked by NoScript.

For more detailed configuration see the **NoScript FAQ (http://noscript.net/faq)**.

uMatrix

uMatrix (https://addons.mozilla.org/firefox/addon/umatrix/) is forked and refactored from HTTP Switchboard. It allows you to selectively block Javascript, plugins or other resources and control third-party resources. It also features extensive privacy features like user-agent masquerading, referering blocking and so on. It effectively replaces NoScript and RequestPolicy. See the **old HTTP Switchboard wiki (https://github.com/gorhill/httpswitchboard/wiki/How-to-use-HTTP-Switchboard:-Two-opposing-views)** for different ways how to use it.

For more Information visit the **project site (https://github.com/gorhill/uMatrix)**.

Cookie Monster

Cookie Monster (https://addons.mozilla.org/firefox/addon/cookie-monster/) is a similar extension to NoScript but will the goal of managing cookies.

From the preferences for Cookie Monster select "Block All Cookies". Once this is done, just as with NoScript, you can enable the use of cookies for specific pages from either the Cookie Monster icon on the toolbar or by right clicking the page and navigating to Cookie Monster. You have the option to accept cookies from the website in question or alternatively to only temporarily allow cookies for the current session.

Cookie AutoDelete

Cookie AutoDelete (https://addons.mozilla.org/firefox/addon/cookie-autodelete/) is an extension that deletes cookies as soon as the tab closes. Supports automatic and manual cookie cleaning modes. (Support for clearing LocalStorage was added in version 2.1, but only for Firefox versions 58+. The same release added support for first part isolation, but only for Firefox versions 59+).

RefControl

RefControl (http://www.stardrifter.org/refcontrol/) is an extension to control what gets sent as the HTTP Referer. Once installed RefControl can be configured so that no referer gets sent when navigating to a new webpage. This prevents the server from knowing which website you originated from.

To do this open RefControl's preferences and change the setting for "Default for sites not listed:" to <Block>.

Note: This extension has not been updated since 2014 and will not work with modern versions of Firefox. However Firefox now has native options to control emitted HTTP referers, possibly replacing plugins such as RefControl and Smart Referer. See **Firefox tweaks#Referrer header control**.

RequestPolicy

RequestPolicy Continued (https://addons.mozilla.org/firefox/addon/requestpolicy-continued/) (a successor to the original **RequestPolicy (https://addons.mozilla.org/firefox/addon/requestpolicy/)**) is an extension for Mozilla browsers which lets you have control over cross-site requests. It also lets you blacklist or whitelist requests by default. Disabling unnecessary cross-site requests leads to better privacy, safety and faster browsing.

Note: This addon is currently **in the process of being updated (https://github.com/RequestPolicyContinued/requestpolicy/issues/704)** for use on modern versions of Firefox (57+).

Decentraleyes

Decentraleyes (https://addons.mozilla.org/firefox/addon/decentraleyes/) protects you against tracking through "free", centralized, content delivery. It prevents a lot of requests from reaching networks like Google Hosted Libraries, and serves local files to keep sites from breaking. Complements regular content blockers.

CanvasBlocker

CanvasBlocker (https://addons.mozilla.org/firefox/addon/canvasblocker/) Blocks or fakes the JS-API for modifying <canvas> to prevent Canvas-Fingerprinting.</canvas>

> **Note:** Mozilla is adding a built-in permission system to allow blocking of HTML5 canvas image track requests, **targeted for release with verion 59 (https://wiki.mozilla.org/Security/Fingerprinting)**.

Random User Agent

Random User Agent (https://addons.mozilla.org/firefox/addon/random-agent-spoofer/) rotates complete browser profiles (from real browsers/devices) at a user defined time interval. It includes many extra privacy enhancing options.

Privacy Settings

Privacy Settings (https://addons.mozilla.org/firefox/addon/privacy-settings/) provides a toolbar panel for easily altering Firefox's built-in privacy settings.

Stop Fingerprinting

Stop Fingerprinting (https://addons.mozilla.org/firefox/addon/stop-fingerprinting/) disables / modifies some browser APIs that would otherwise allow browser fingerprinting. However, this addon is not compatible with newer versions of Firefox (57+).

Remove system-wide hidden extensions

Several extensions, hidden to the user, are installed by default in `/usr/lib/firefox/browser/features`. Many can be safely removed via `rm extension-name.xpi` in order to completely remove unwanted features. Many of these extensions are not enabled by default and have a menu option for enabling or disabling. Note that any files removed will return upon update of the **`firefox (https://www.archlinux.org/packages/?name=firefox)`** package. Below are a few examples of these extensions and their features.

- `activity-stream@mozilla.org.xpi` - "Activity Stream" which replaces the new tab page. See **[4] (https://github.com/mozilla/activity-stream)**
- `firefox@getpocket.com.xpi` - **Pocket (https://getpocket.com/firefox/)**

- `followonsearch@mozilla.com.xpi` - Search telemetry. See also **#Disable telemetry**.
- `shield-recipe-client@mozilla.org.xpi` **SHIELD studies (https://support.mozilla.org/en-US/kb/shield)**

See also **[5] (https://dxr.mozilla.org/mozilla-release/source/browser/extensions/)** for a full list of system extensions including README files describing their functions.

Retrieved from "https://wiki.archlinux.org/index.php?title=Firefox/Privacy&oldid=507317"
