

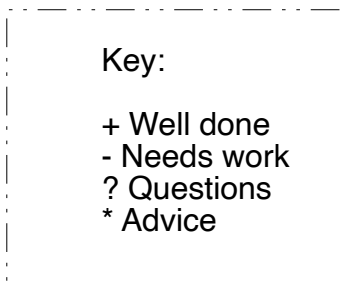
JShelter UX Review

Plaintext Design – Susan Farrell

December 2022

About This Report

This usability review starts with finding the JShelter add-on on Firefox’s website. Then, the user experience is described from looking at docs, preferences, toolbar menu, and briefly, the website.



About JShelter

“JShelter focuses on fingerprinting prevention, limitations of rich web APIs, prevention of attacks connected to timing, and learning information about the device, the browser, the user, and surrounding physical environment and location.” From <https://arxiv.org/abs/2204.01392>

* Although this explanation is succinct, that’s a very long sentence, and it doesn’t unpack “fingerprinting” or “limitations of rich web APIs.” It would be great if these terms were explained in the information users are likely to read while first encountering JShelter.



Install Firefox Add-On

<https://addons.mozilla.org/en-US/firefox/addon/javascript-restrictor/>

+ Great reviews (4.6 stars)(25)

+ Pretty good “About this extension” information, and it provides links

+ “Report a bug” exists


+ Was updated only months ago

– “Not actively monitored for security by Mozilla” (Can you put an audit link on this page?) 


– Only 518 users

– Bug reporting can be done only by those who can use dev tools like GitHub?

– Release notes don't make sense 

– Description isn't illuminating: “JShelter controls the APIs provided by the browser. The goal is to improve the privacy and security of the user running the extension.” 



* What the two browser websites (Firefox and Chrome) tell people about the extension is slightly different, and that might account for some of the difference in installs. Migration to Chrome and the increasing Firefox privacy controls might account for more. 

– Chrome does notify on install that JShelter can access and alter all websites, but Firefox makes permissions sound like more is going on, right on the extension page surface:

Firefox extension: 

This add-on needs to:

- Display notifications to you
- Access browser tabs
- Access browser activity during navigation
- Access your data for all websites





This add-on may also ask to:


- Clear recent browsing history, cookies, and related data

+ Chrome extension extension page surface:

- The publisher has disclosed that it will not collect or use your data.

* Advice for increasing installs:

- Try to get on these pages: <https://addons.mozilla.org/blog/top-anti-tracking-extensions/>
<https://addons.mozilla.org/en-US/firefox/collections/4757633/privacy-matters/> 
- Compare your information format with DDG's and try to emulate the good things about theirs:
<https://addons.mozilla.org/en-US/firefox/addon/duckduckgo-for-firefox/>
- Participate in discussions on Reddit, especially here:
<https://www.reddit.com/r/PrivacyGuides/> 
- Suggestion for the short description: “JShelter improves your privacy and security by putting you in control of browser ‘fingerprinting’ and geolocation on websites that seek to identify you.” 
- It seems that JShelter got a lot of attention when FSF announced it. It would be great to get more good press, for example, positive mentions on Twitter, a security/privacy blog post or podcast. Consider trying to be a guest on Smashing Security, Risky Biz, or Cyber to talk about JShelter after the redesign. Try to get EFF’s endorsement and/or a Wired article. 

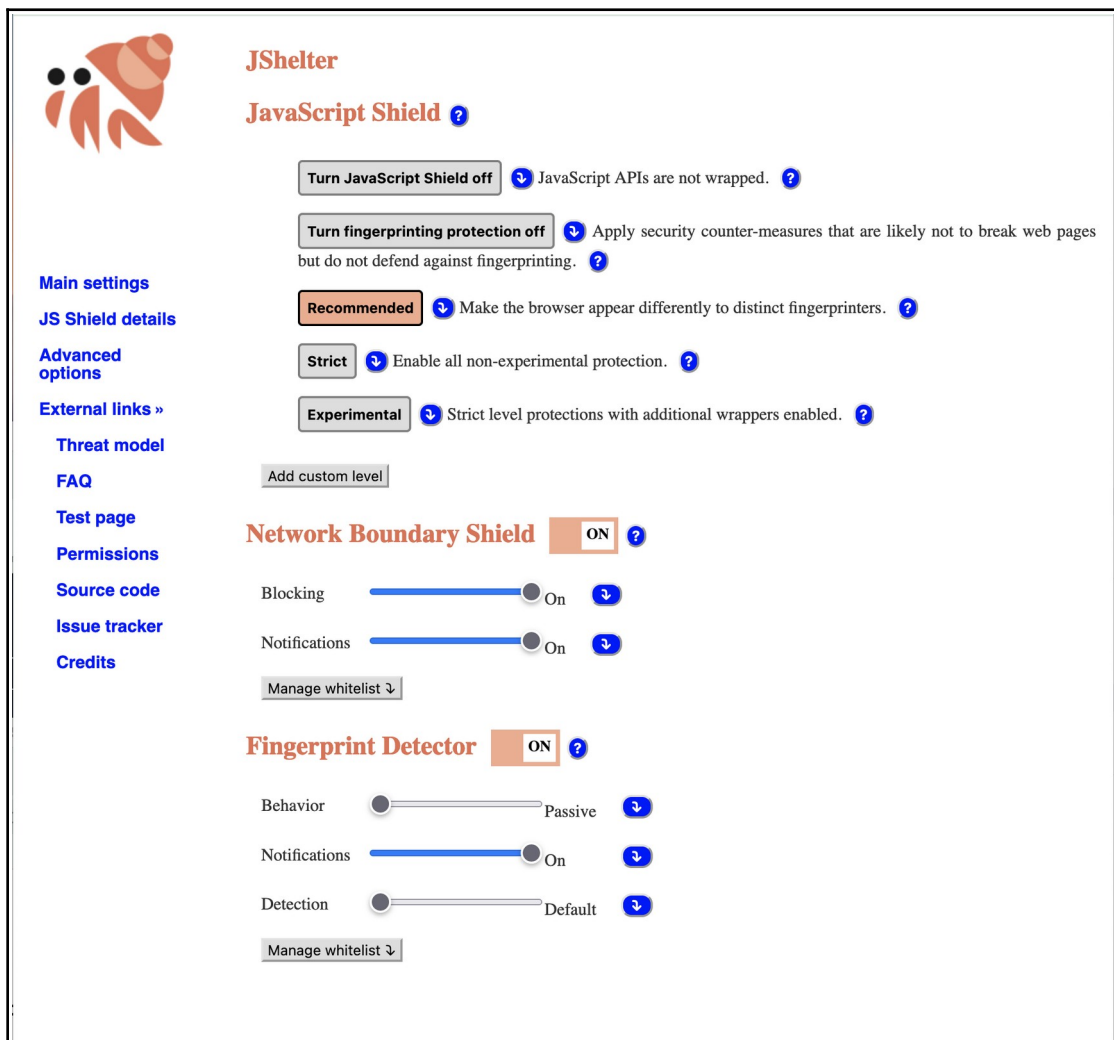
* Suggestions for the Firefox *About this extension* page: 

- Simplify the language and sentence structure on this page.
- Add a bullet list of features + benefits and put it between “What is JShelter” and “How does it work?”
- Assume people won't go to the FAQ to find out whether they want it or not. What else must they know here? Copy that or deep link to the FAQ from this page.
- Make relnotes understandable. These are fixes or new features, right? Start with “Fixed:” and/or “New feature:”. Consider linking to the relnotes so you have room for more explanations. See DDG’s page for contrast.

- Developer comments: Add Support email or form to this.
- Add Privacy Policy link – This extension wants access to everything, so reassure people prominently about your own data collection practices.
- Add social proof – You have backing from FSF and at least one famous developer. Use those associations to instill confidence. This social proof should also be in the FAQ under “Why should you trust us?”
- Reassure people that your extension adds value over others they might use, explain that yours plays nice with theirs, and list the ones you recommend to use together, here or via a link, in the FAQ.
- Make sure your tool doesn't break PayPal, reCaptcha, and YouTube, as reviewers stated that it does. Add to FAQ and site-specific info in the extension, if needed. Consider ways to make user decisions about settings for these sites a lot simpler.
- Ensure that answers to these questions are in the FAQ:

[https://www.reddit.com/r/privacy/comments/q1671p/
fsf announces jshelter browser addon to combat/](https://www.reddit.com/r/privacy/comments/q1671p/fsf_announces_jshelter_browser_addon_to_combat/)

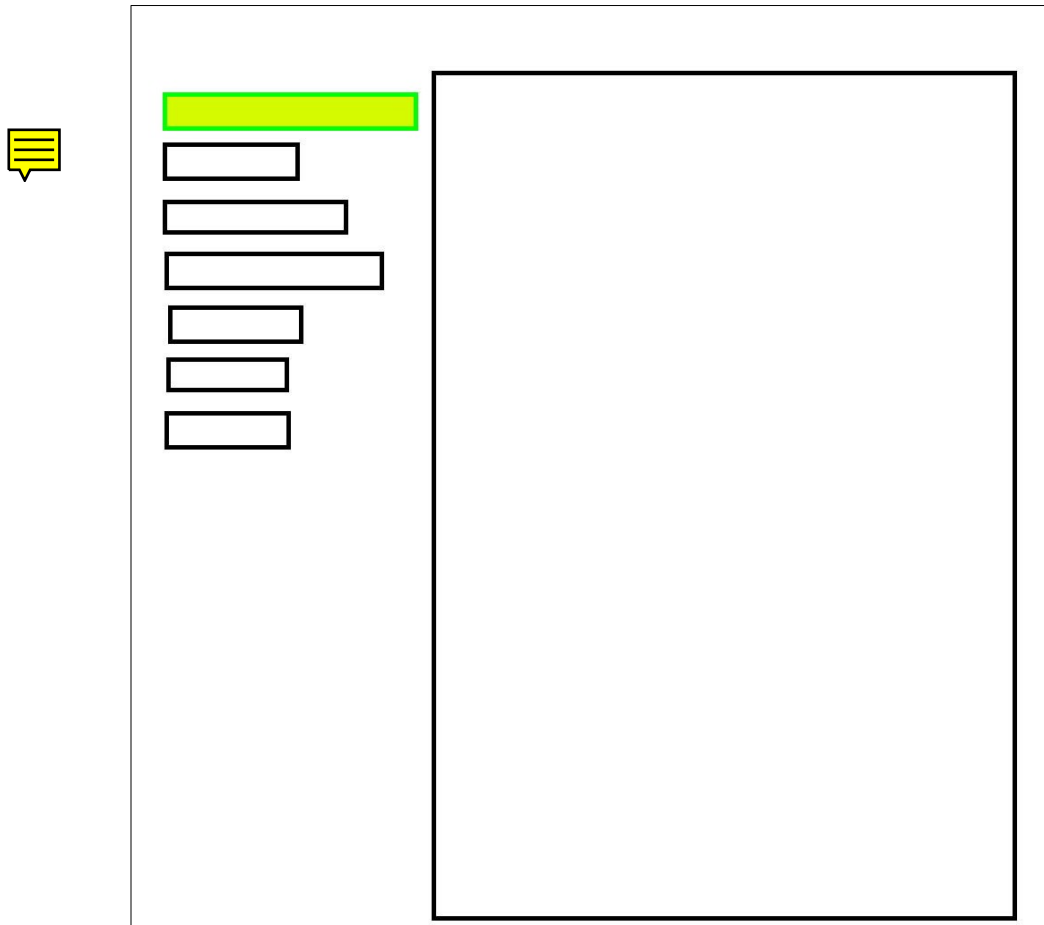
Firefox Jshelter Preferences



Firefox preference page, defaults after installation, before redesign.

- + Help icons lead to help.
- + Help is on this page not on a different page.
- + Help offers drill-down to more help on the website.
- + Website table of contents provides easy access to important information.
- + Recommended, Strict, and Experimental settings are provided so users don't have to make dozens of decisions if they don't want to.

After discussions with the developer, I recommended that this formerly confusing panel, above be constructed in a way that shows both that it represents exclusive choices and that these choices change the sliders. Instead of showing all the permutations, the choices would be reflected in one panel that changes with the selected option on the left.



– When Recommended, Strict, and Experimental buttons are pressed, they show no change if the mouse is still over the button, which is extremely confusing and leads to lots of clicking that seems to do nothing. Experimental clicking to try to affect the button state adds to the feeling that this thing isn't really working.

* Fix the interaction design by removing the hover state for the buttons, so that the button reacts to clicks regardless of mouse positioning.

– There are many spelling mistakes in the help text, which undermines user confidence in the quality of the application.

– Explanations are very technical, which might lead people to dismiss them all after encountering material they can't understand, for example: "JavaScript APIs are not wrap"

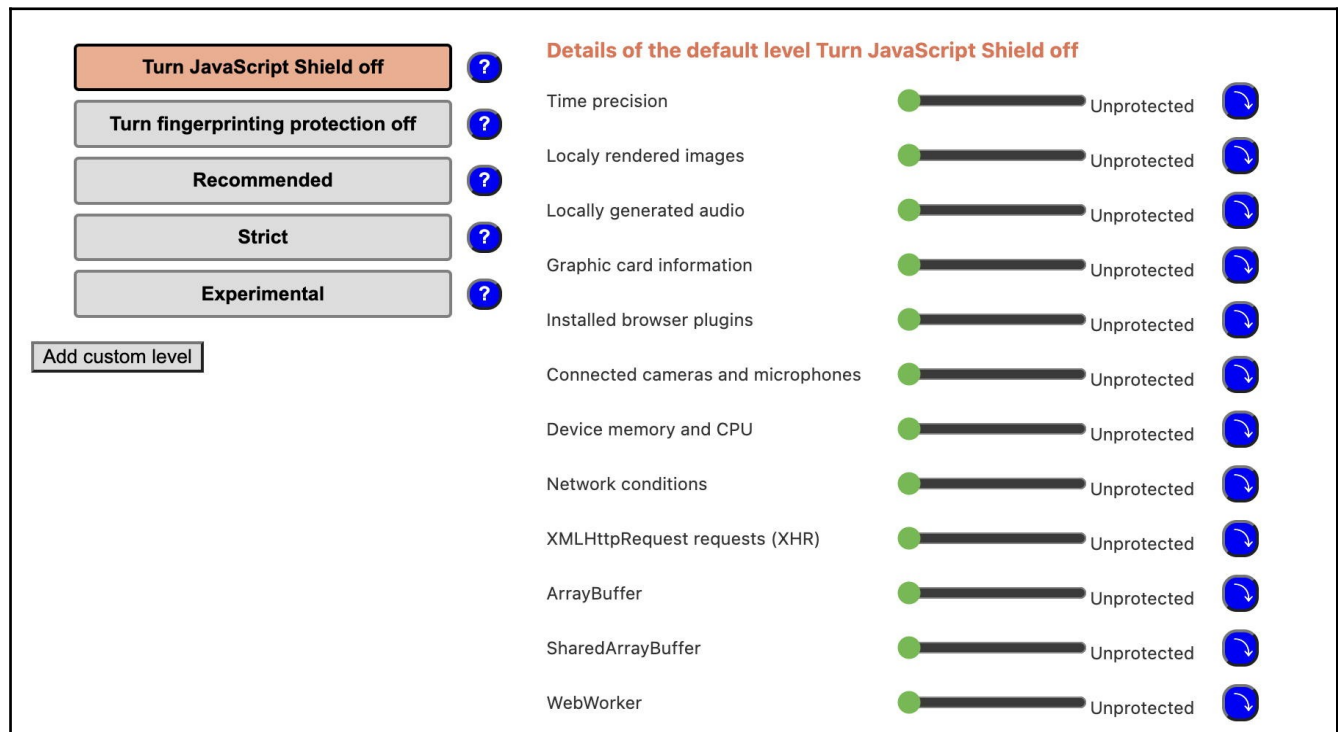
? What is API wrapping and why would the user care?

– The button design seems idiosyncratic and a bit rough. It's also inconsistent (rounded, square, flat, beveled, raised, half-dropshadow). (Fixed)

– Sliders don't line up with the indicator text well. (Improved)

- Some word spacing is odd in the expanded sections, as if the text is fully justified, so words are farther apart than normal.
- "Whitelist" is being used, even though it's now preferred that these be "Allow list" / "Block list" to avoid racial good/bad metaphors.
- The help text (under the (?)s) is confusing and at a very high technical reading level. It's easy to decide that this tool is too complicated to use.
- The help text refers to "use this level," but there are no levels, only *On* and *Off*. Also, it's not clear what "this" refers to, the current state, or the state obtained if the instruction on the button is followed.

Improved Designs



The redesigned panel (partially shown above) shows the choices on the left and the effects on the right. Hovering the mouse over a choice button causes the right side to showing how the sliders would change. Now it's much easier to understand the effects of your choice and to understand that the choices are exclusive, rather than additive.

- The words: "details of the default level Turn JavaScript Shield off" are difficult to understand.

* Given that all the sliders are showing unprotected and are not movable, I would expect this text to say "JavaScript Shield is off. Details:" Same for the fingerprinting protection. Similarly:

- Recommended level, details:
- Strict level, details:
- Experimental level, details:



?

?

?

?

?

Details of the default level Turn fingerprinting protection off

Time precision		High	<input type="button" value="↺"/>
Locally rendered images		Unprotected	<input type="button" value="↺"/>
Locally generated audio		Unprotected	<input type="button" value="↺"/>
Graphic card information		Unprotected	<input type="button" value="↺"/>
Installed browser plugins		Unprotected	<input type="button" value="↺"/>
Connected cameras and microphones		Unprotected	<input type="button" value="↺"/>
Device memory and CPU		Unprotected	<input type="button" value="↺"/>
Network conditions		Strict	<input type="button" value="↺"/>
XMLHttpRequest requests (XHR)		Unprotected	<input type="button" value="↺"/>
ArrayBuffer		Unprotected	<input type="button" value="↺"/>
SharedArrayBuffer		Unprotected	<input type="button" value="↺"/>
WebWorker		Strict	<input type="button" value="↺"/>
Physical location (geolocation)		Town	<input type="button" value="↺"/>

When the second button is chosen, the right panel changes to reflect the changed parameters.

JavaScript Shield ?

?
 ?
 ?
 ?
 ?

[Main settings](#)
[JS Shield details](#)
[Advanced options](#)
[External links »](#)
[Threat model](#)
[FAQ](#)
[Test page](#)
[Permissions](#)
[Source code](#)
[Issue tracker](#)
[Credits](#)

Details of the default level Recommended

Time precision	High		
Locally rendered images	Little lies		
Locally generated audio	Little lies		
Graphic card information	Little lies		
Installed browser plugins	Fake		
Connected cameras and microphones	Add fake		
Device memory and CPU	Low		
Network conditions	Strict		
XMLHttpRequest requests (XHR)	Unprotected		
ArrayBuffer	Unprotected		
SharedArrayBuffer	Unprotected		
WebWorker	Strict		
Physical location (geolocation)	Town		
Physical environment sensors	High		
User idle detection	Deny access		
Idle period task scheduling	Little lies		
Gamepads	Strict		
Virtual and augmented reality devices	Strict		
Multimedia playback	Unprotected		
Unreliable transfers to server (beacons)	Disabled		
Hardware battery	Disabled		
Persistent identifier of the browser tab	Strict		

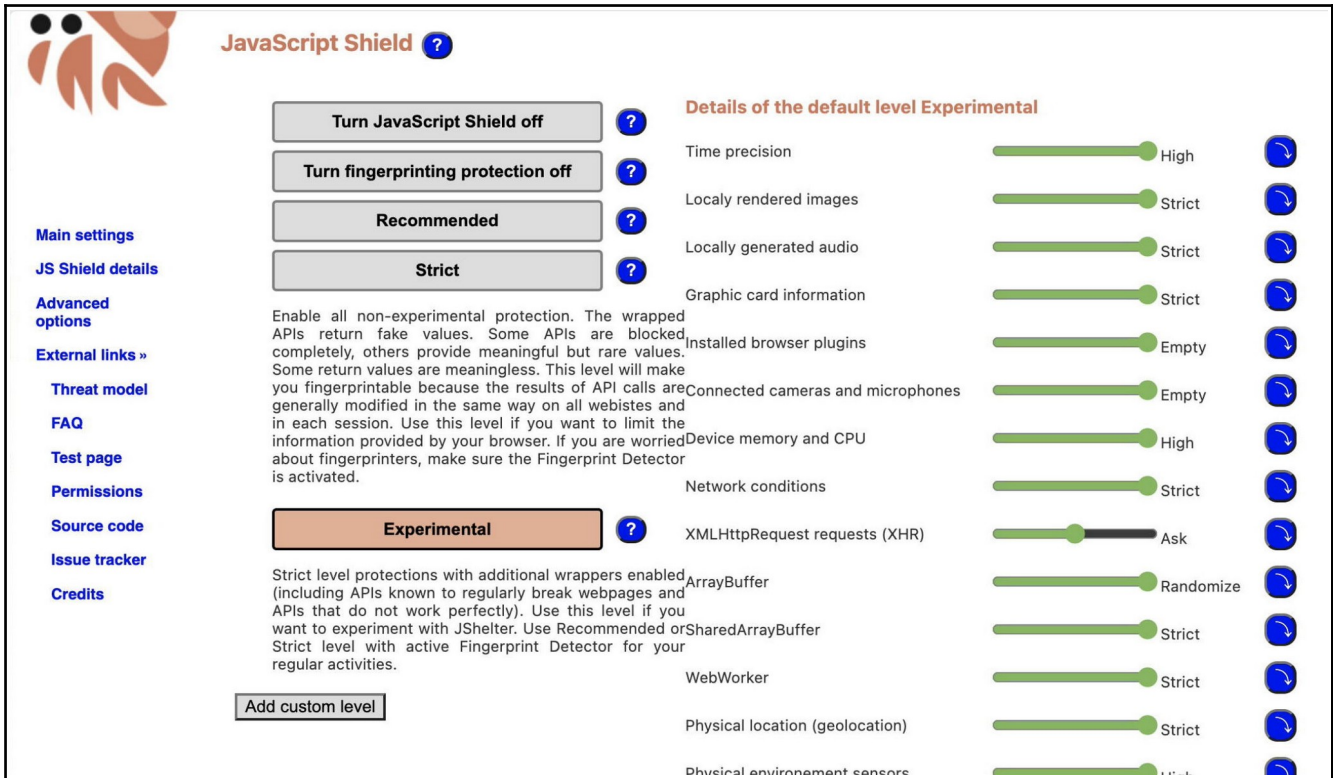
Network Boundary Shield **ON** ?

Blocking On
 Notifications On

Fingerprint Detector **ON** ?

Behavior Passive
 Notifications On
 Detection Default

This longer view of the new configuration page shows the result of choosing “Recommended” level of protection.



JavaScript Shield ?

?
 ?
 ?
 ?
 ?

Enable all non-experimental protection. The wrapped APIs return fake values. Some APIs are blocked completely, others provide meaningful but rare values. Some return values are meaningless. This level will make you fingerprintable because the results of API calls are generally modified in the same way on all websites and in each session. Use this level if you want to limit the information provided by your browser. If you are worried about fingerprinters, make sure the Fingerprint Detector is activated.

Details of the default level Experimental

Time precision	High	?
Locally rendered images	Strict	?
Locally generated audio	Strict	?
Graphic card information	Strict	?
Installed browser plugins	Empty	?
Connected cameras and microphones	Empty	?
Device memory and CPU	High	?
Network conditions	Strict	?
XMLHttpRequest requests (XHR)	Ask	?
ArrayBuffer	Randomize	?
SharedArrayBuffer	Strict	?
WebWorker	Strict	?
Physical location (geolocation)	Strict	?
Physical environment sensors	...	?

Help text (which opens when you click on a (?)), still needs a bit of work on layout spacing, but it has good advice about when to choose which level and how to stay protected.



Add New Level



JShelter

Note that for fingerprintability prevention, JShelter does not wrap objects that are not defined.

Your browser does not support:

- VRFrameData.prototype.timestamp.
- Sensor.prototype.timestamp.
- OffscreenCanvas.prototype.convertToBlob.
- Navigator.prototype.deviceMemory.
- Navigator.prototype.connection.
- window.NetworkInformation.
- window.SharedArrayBuffer.
- Magnetometer.prototype.x.
- Magnetometer.prototype.y.
- Magnetometer.prototype.z.
- Accelerometer.prototype.x.
- Accelerometer.prototype.y.
- Accelerometer.prototype.z.
- Gyroscope.prototype.x.
- Gyroscope.prototype.y.
- Gyroscope.prototype.z.
- OrientationSensor.prototype.quaternion.
- AmbientLightSensor.prototype.illuminance.
- window.IdleDetector.
- IdleDetector.requestPermission.
- IdleDetector.prototype.screenState.
- IdleDetector.prototype.userState.
- Navigator.prototype.activeVRDisplays.
- Navigator.prototype.xr.
- Navigator.prototype.getBattery.
- window.BatteryManager.
- window.NDEFMessage.
- window.NDEFReader.
- window.NDEFRecord.

Add new level

Name:

Description:

Time precision Unprotected 

Unprotected

Prevent attacks and fingerprinting techniques relying on precise time measurement (or make them harder).
Limit the precision of high resolution time stamps (Date, Performance, events, Gamepad API, Web VR API).
Timestamps provided by the Geolocation API are wrapped as well if you enable Geolocation API wrapping

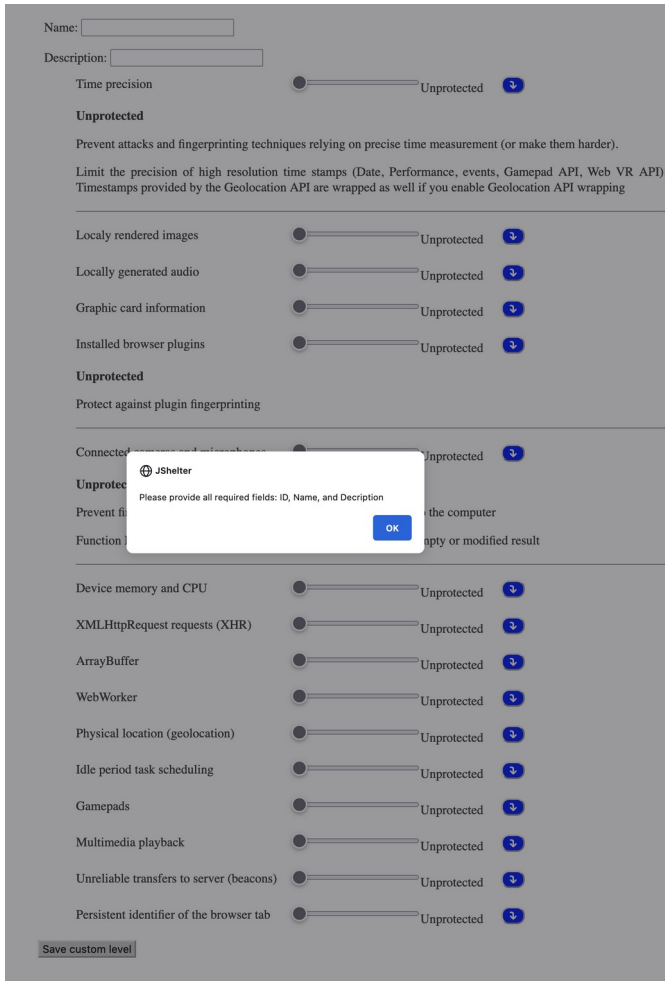
Locally rendered images Unprotected 

Locally generated audio Unprotected 


Graphic card information Unprotected 

Installed browser plugins 


“Add new level”, expanded options (before redesign)




Before the redesign, experimental clicking on Custom level forced the user to make a choice rather than allowing them to back out safely.

 Note: Some or all of the issues mentioned below about the screen above are being addressed currently, but I'm not sure exactly which ones.

+ Changing a slider changes the help text *if that's displayed*.

* Expand the help text when a user interacts with the slider, so they can have the value of the explanation while in the process of deciding. 

– “Add new level” is confusing. Pressing the button shows the information in the image above, plus a few more options and a button at the bottom.

– After you press “Add new level” there is no Cancel option, only “Save custom level,” so you can't exit this operation without doing something. (Improved) 

? “New level” of what?

? What are these things and which are most important?

? How can I find out what fingerprinting is about and why I would care?

? Does my description need to be like the ones shown on the green list?

? What are the effects of changing these parameters?

? Why are these all off?

? Why are Fingerprint Detector and Fingerprinting protection not adjacent?

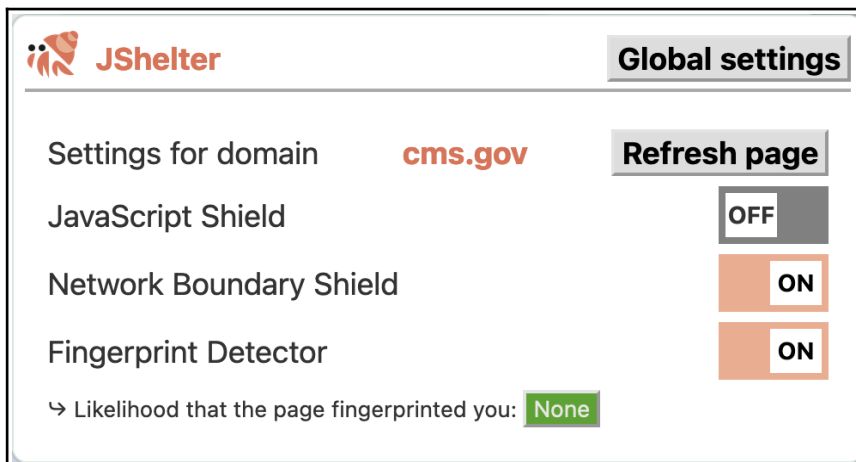
– Attempting to exit the Add new level action means pressing “Save custom level” because there is no Cancel or Back. (Fixed)

– Pressing the button causes an error message whose only option is “OK”.

– The error message demands “ID, Name and Decription” (spelling mistake), but only Name and Description fields are present. There seems to be no way to add ID, even if you knew what that was.

– This custom-level operation apparently calls for changing some parameters, adding a name and description, and saving that, but there are no instructions for doing it.

Firefox toolbar control panel



Firefox toolbar control panel

+ The controls look simple and there are only a few of them.

* Add contextual help to define the terms that links to more information.

+ These toggle switches follow best practices in terms of color around the buttons and labels and colors that reflect the state.

+ Global settings can be accessed from here.

+ Global settings opens a new page *or* switches to the page if open.

– These controls do not follow OS style guidelines for MacOS or seem to conform to Firefox styles.

- Place labels closer to the controls.
- Use a grid for alignment of UI elements. If things can line up, they should.

- Global settings is an action button, but it should probably be a link, since it displays a new page. It should probably also be renamed “Main settings” to match the menu on the settings page.
- “None” seems like a state indicator, but it’s rendered as an action button. In fact it is an action button as it opens a blank report that reports “None” and nothing.
 - When there’s no report, just indicate the state as “None,” but don’t show a button that goes to nothing. Rename the button “View report” when there is content in the report, and if it’s important, say something about what was found, or add an alert icon and alt text to call attention to it.
 - Don’t use gray for active action buttons. Gray means “inactive” or “unavailable” in UI design language. Choose another color and use it for “Review Report” as well.

JShelter Global settings

Settings for domain **583b6649-2b1f-474a-982a-1d6c1e41632f** Refresh page

JavaScript Shield OFF

Network Boundary Shield ON

Fingerprint Detector ON

↳ Likelihood that the page fingerprinted you: **None**

- Precision reduction: The original value is too precise and it is not necessary for most use cases. JavaScript modifies the values so that typical and benign use cases are not affected.
- Provide fake information: Some wrappers provide fake information mostly to confuse fingerprinters. For example, canvas wrappers modify the image so that the same instructions produce different result in each session each domain.
- Hide information: Some APIs provide information that is not generally needed and can be hidden from most pages. Depending on the API, JavaScript Shield might return an error, an empty value, or block it completely.

See our blog post for more information on [browser fingerprinting counter-measures](#) and [farbling](#).

Turn JavaScript Shield off [?] [?]

JavaScript APIs are not wrapped. Use this level if you (1) trust the operator of the visited page(s) and you v give them access to full APIs supported by the browser, or (2) if you do not like JavaScript Shield but yo to apply other protection mechanisms.

Time precision	Unprotected	[?]
Locally rendered images	Unprotected	[?]
Locally generated audio	Unprotected	[?]
Graphic card information	Unprotected	[?]
Installed browser plugins	Unprotected	[?]
Connected cameras and microphones	Unprotected	[?]
Device memory and CPU	Unprotected	[?]
XMLHttpRequest requests (XHR)	Unprotected	[?]
ArrayBuffer	Unprotected	[?]
WebWorker	Unprotected	[?]

When opening the toolbar menu from the Settings page, it’s difficult to determine the state of protection.



– When the toolbar menu is open while on the settings page, the JavaScript Shield appears to be both off and on. As a result the user may worry that this extension doesn't work or that it's so confusing that they can't determine whether it's on or not.



Some overall advice for the extension

* Rewrite all the help text, explaining both states in user-facing language (what On does and why you might want it; what Off does and why you might want that). A UX writer or technical copy-editor can make all the difference. They could also very usefully edit the website text and Add-on page at Firefox.



* Provide obvious and unambiguous on/off switches. The toggle switches and sliders are clear, but the buttons are not. On/Off toggle buttons have failed in UIs since they were first introduced because of ambiguity (Do you press On to turn it on or On to turn it off? Is it a command or a state indicator?). The toggle sliders are much better at indicating their current state visually.



* Add a summary at the top about what the extension does for you, the user. Explain that these defaults should be good, but if you've trouble with X, what to change.



* Never use color to indicate anything important, because many people don't perceive color. Use text, icons or symbols, light/dark contrast, and position to indicate, and use color to decorate and add emphasis for those who can see it.



* Ensure that the default settings are the best configuration option for the most people, and reassure people about that so they won't play with the controls unnecessarily, possibly making their usability or privacy/security worse.



* Provide brief decision support in help text for users on this page and provide technical explanations for security pros and devs on the website via links from the help text. ("Technical details about API wrapping", etc.)



* Consider adding presets to the page-specific controls in the toolbar, so when the user has a problem with a page, they can easily try options like "recommended settings," "my settings," turning likely suspects off, or resetting to previous parameters. Help people decide what to turn off first.



WEBSITE

<https://jshelter.org/>

I looked at some of the key pages: Home, Frequently Asked Questions, Install, and Blog, as a curious new user might, to get the gist of the extension. I did not review the whole site.

+ The website offers information about the extension and serves as decision support for installing or not installing.

+ The website looks professional and contains extensive information about the tool.

+ The website shows good social proof in terms of its funding and developers.

+ The website seems to have information that's both transparent and helpful.

<https://jshelter.org/faq/>

+ The frequently asked questions (FAQ) seem like good questions that users might ask.

- + The FAQ answers many questions about recommended settings and companion extensions.
- + The FAQ suggests reading the threat model.
- + The FAQ uses highlighting for key information and supports visual scanning in its use of bold headings for the questions.

– Typo? “The NoScript Suite main developer is a part of the JShelter team, and JShelter shares a lot of code with Jshelter.”

“We understand that our users do not want to easily give information about their devices. Hence, we suggest having JavaScript Shield active on fingerprinting sites. It is up to you if you want to provide as little information as possible (Strict level), want to have a different fingerprint every visit (Recommended level, keep in mind that you are providing your login, so your actions are linkable), or you want to create your own level.”

– This advice complicates a common use case, which is “I want to access my bank safely.” On the one hand, you seem to advise strict settings, but on the other, you explain why recommended settings defeat the purpose of using those settings when visiting a site that fingerprints you and that you must log into. This undermines “recommended” and causes people to have to choose between complexity and access.

* Consider whether it would be possible to have recommended settings be different for sites that fingerprint you that you must log into and in that case, provide an alert and easy switch to set for those from the browser toolbar.

“Test yourself on common fingerprinting testers that the Strict level considerably lowers the information about your computer.”

– This text is confusing.

* Perhaps it means: Test your browser on common fingerprinting testers. Then use the Strict level and test again to see that it considerably lowers information about your computer.

* Cover the question: Can I run Firefox fingerprinting protection (FFP) resistFingerprinting with JShelter? The first mention doesn't make that clear, and the second doesn't explain how to do it.

* Fix the typo: resistFingerprining (missing T, at least twice in the FAQ and maybe other places on the website)

* Repeat the steps (shown now under the popup window FAQ) how to access about:config in the resistFingerprinting FAQ, because this process is not officially supported on Firefox's website and is now hard to find, and some people won't read through the whole FAQ.

– Even though it's not your problem, the setting for resistFingerprinting in about:config is hard to understand, so anyone using it might choose a poor configuration (boolean, number, string +(add)). When I looked at my settings, they were set to Strict and yet the about:config setting showed the +(add), so it wasn't clear from there whether it was set to be on or not.

* Explain how to set resistFingerprinting in about:config briefly when recommending turning it on (in regard to fingerprinting and fonts in the FAQ). Fingerprinting seems to be a blanket setting under Preferences: Enhanced Tracking Protection: Strict, so maybe that's the place to point people instead.

* Use in-page links rather than “See above” when the information is more than a few inches away.

* Explain what “little lies” is.

* Consider renaming “strict to stable” since it apparently means stable, not strict.

* Add a table of contents with jump links to the FAQ.

<https://jshelter.org/install/>

+ This page links to locations for getting the extension.

<https://jshelter.org/blog/>

+ The blog shows activity in recent months.