

Simple Analytics

This pdf is generated on April 15, 2021. Go to [the documentation page](#) for the most up-to-date version.

Content Security Policy version

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement to distribution of malware. [Read more on CSP at MDN.](#)

For Simple Analytics you want to add the following Content Security Policy header (we included `'self'` for all as well):

```
Content-Security-Policy: script-src 'self'  
https://scripts.simpleanalyticscdn.com; connect-src 'self'  
https://queue.simpleanalyticscdn.com; img-src 'self'  
https://queue.simpleanalyticscdn.com;
```

Alternatively, the element can be used to configure a policy, for example:

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self'  
https://scripts.simpleanalyticscdn.com; connect-src 'self'  
https://queue.simpleanalyticscdn.com; img-src 'self'  
https://queue.simpleanalyticscdn.com;">
```

Basically we use <https://scripts.simpleanalyticscdn.com> for our public script, <https://queue.simpleanalyticscdn.com> to send Beacon API data and error requests, and we use <https://queue.simpleanalyticscdn.com> also for sending data through our pixel.

Don't forget to add your own assets to the above Content Security Policy.

This pdf is generated on April 15, 2021. Go to [the documentation page](#) for the most up-to-date version.