Reconciling Content Security Policy With Google Analytics and Google Tag Manager

Content Security Policy (CSP) is a web standard providing protection from third-party assets such as cross-site scripting attacks (XSS) that may cause serious security concerns. CSP describes safe sources, establishes rules of use of built-in styles and scripts as well as dynamic assessment of JavaScript. Loading from resources not on the so-called "white list" is blocked.

CSP for Google Analytics

Google Analytics can use 2 - 4 features often restricted by Content Security Policy, so your task is to enable them.

JavaScript

The first thing you should do is configure the script-src directive to allow Google Analytics to run JavaScript.

- Add *https://www.google-analytics.com* to the source list of your script-scr directive.

Note: the https is optional, while the www is mandatory.

- Add the Google Analytics code snippet to your page.

+44 20 7183 5820
info@magora.co.uk
sales@magora.co.uk

Note: This is an inline snippet, known as **function(i,s,o,g,r,a,m)**, which is restricted by CSP.

Here are 3 ways you can run Google Analytics from less secure to more reliable:

1. Add the string *'unsafe-inline'* to the script-scr directive source list to allow all inline snippets to run. This is the least secure way as unsafe code also gets a let-pass.
2. Move the Google Analytics part of the code to an external code file hosted on a whitelisted domai n, for example on your website primary domain.
3. Opt for use of nonce-value on the inline script. This way is most secure, but also complicated, so choose it only if nonce-values are already used for other inline scripts.

Tracking Beacons

Content Security Policy may restrict the ways Google Analytics sends data to servers for Post requests, Image requests and the browser "Beacon" feature.

- Whitelist Google Analytics by adding *https://www.google-analytics.com*
- Add *https://stats.g.doubleclick.net* and *https://www.google.com* to the source list if AdWords integration or Advertising Features is enabled.

Examples

Here is a simple policy enabling Google Analytics to function without the AdWords or Advertising features. It allows only what is strictly necessary and restricts other non-Google resources.

default-src *'self' https://www.google-analytics.com 'unsafe-inline'*

This way you can move the Google Analytics code snippet to a separate file as this policy requires. It is hosted on the same domain as the main site.

script-src *'self' https://www.google-analytics.com;*

connect-src *https://www.google-analytics.com www.google-analytics.com https://stats.g.doubleclick.net*

img-src *https://www.google-analytics.com www.google-analytics.com https://stats.g.doubleclick.net.*

Google Tag Manager

Content Security Policy may also restrict some assets loaded on your page by Google Tag Manager.

JavaScript

Tag Manager is a script-injection framework that dynamically loads JavaScript sections onto your page, so you can't restrict it from executing inline snippets as it works with Google Analytics. To make Tag Manager function, you should:

+44 20 7183 5820
info@magora.co.uk
sales@magora.co.uk

- *Update your script-src (or default-src) directive with* https://www.googletagmanager.com and *'unsafe-inline'* in the source list.

Other Assets

If you need to load some third-party tracking pixels, you should work out how to allow the appropriate script or image sources.
Trial and error is the most efficient method here:

- Add the tracking code in Tag Manager,
- Make a preview,
- And then monitor the error message about Content Security Policy.

Summary

Content Security Policy is a helpful feature for reinforcing your site security. With some coordination and minimal effort, it can work perfectly in conjunction with Google Analytics, while Google Tag Manager will require more attention on your part to manage which assets should be allowed. Don't be of afraid of loosing some CSP benefits, as even with Google Tag Manager inline snippets permitted, Content Security Policy still offers considerable security benefits.

+44 20 7183 5820
info@magora.co.uk
sales@magora.co.uk