Specify CSP to Prevent or Minimize the Risk of Security Threats

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v7.4.11 up to v8.2.1.x

EFT v8.0 and later store Advanced Properties in a JSON file. When you upgrade from EFT v7.4.x to EFT v8, the non-default settings that you have defined in the registry will be added to the Advanced Properties file during upgrade. (Default settings become part of the EFT configuration files.) For a more on how to use advanced properties, and a spreadsheet of the advanced properties, please refer to the "Advanced Properties" topic in the help for your version of EFT.

DISCUSSION

The Content Security Policy (CSP) HTTP response header declares which dynamic resources are allowed to load in the browser.

By default, EFT will issue the following CSP header:

Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data:;

These values have the following meanings, as documented here: https://content-security-policy.com/.

default-src 'self' = default policy for loading content

'unsafe-inline' = allow use of inline source elements such as style attribute, onclick, script tag bodies, javascript: URIs

'unsafe-eval'= allows unsafe dynamic code evaluation such as JavaScript eval()

CUSTOM CSP HEADER

You can add additional values, such as “script-src” and “style-src”, by overriding the default CSP header via the registry or as an Advanced Property:

<u>In EFT v8 and later:</u>

Add the name:value pair to the AdvancedProperties.JSON file in EFT's \ProgramData\

directory as described in the "Advanced Properties" topic in the online help for your version of EFT.

```
{
"CSPHeaderOverride": "default-src 'self'; font-src *;img-src * data:; script-src *; style-src *;"
}
```

(Double quotation marks " around the value is required.)

In versions prior to v8.0:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GlobalSCAPE Inc.\EFT Server 7.4\

Key Type: STRING

Key name: CSPHeaderOverride

Values: Provide the new CSP header string. For example:

default-src 'self'; font-src *;img-src * data:; script-src *; style-src *;

You do not need to restart the EFT server service for the new CSP to take effect.

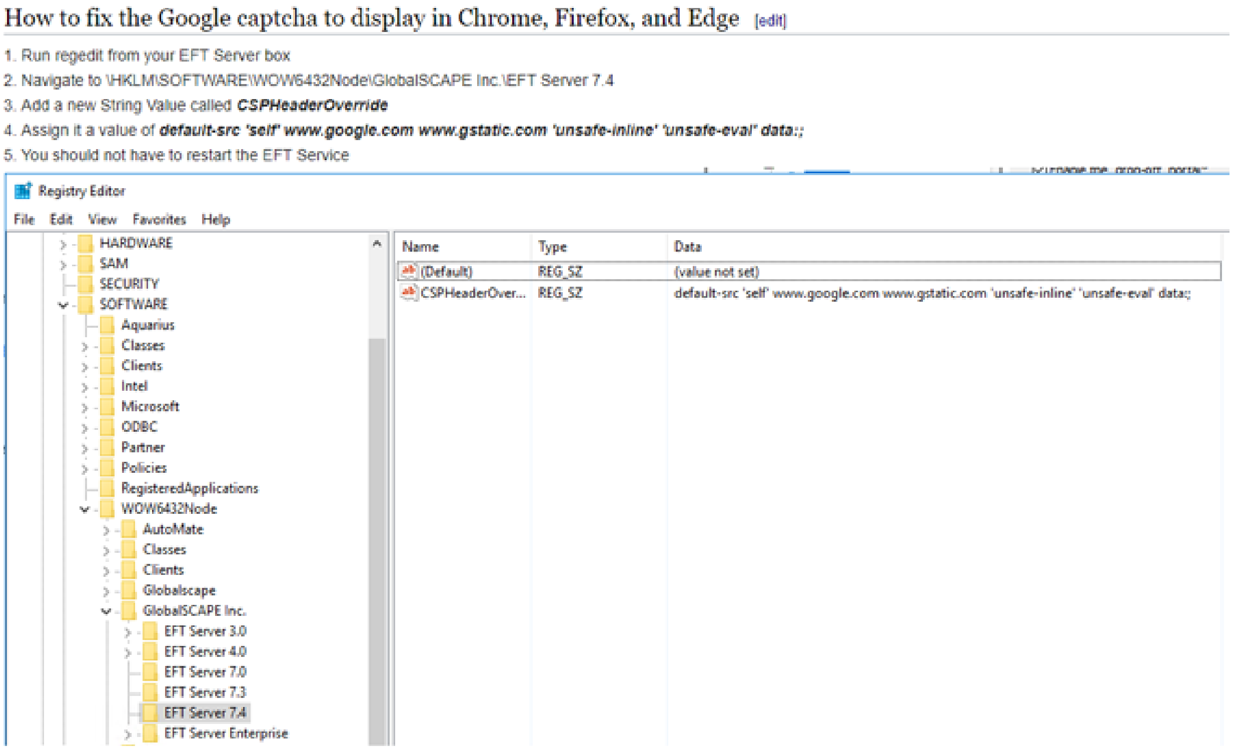
CSP WHEN reCAPTCHA IS USED FOR DROP-OFF PORTAL:

If you enable Google reCAPTCHA for the Drop-off portal, you will need to modify the allowed CSP domains to also include google.com and gstatic.com. This is necessary so that Google’s reCAPTCHA service will work.

Change CSPHeaderOverride to:

> **default-src 'self' www.google.com www.gstatic.com 'unsafe-inline' 'unsafe-eval' data:;**

- If you disable reCAPTCHA, you should consider removing the override so that the default CSP is used. (This setting has no effect in Internet Explorer.)



How to fix the Google captcha to display in Chrome, Firefox, and Edge [edit]

1. Run regedit from your EFT Server box
2. Navigate to \HKLM\SOFTWARE\WOW6432Node\GlobalSCAPE Inc.\EFT Server 7.4
3. Add a new String Value called ***CSPHeaderOverride***
4. Assign it a value of ***default-src 'self' www.google.com www.gstatic.com 'unsafe-inline' 'unsafe-eval' data:;***
5. You should not have to restart the EFT Service

Name	Type	Data
(Default)	REG_SZ	(value not set)
CSPHeaderOver...	REG_SZ	default-src 'self' www.google.com www.gstatic.com 'unsafe-inline' 'unsafe-eval' data:;

Note: As of v8.3.0 EFT now supports Content Security Policy (CSP) level-3 "strict-dynamic" without making any modifications.

Review EFT Release Notes: [EFT Release Notes]

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11435/Specify-CSP-to-Prevent-or-Mi...