

## Specify CSP to Pass Security Web Scans and to use Google reCaptcha for Drop-Off

### THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v7.4.11 and later

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:

In EFT v8 and later:

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

## Specify CSP to Pass Security Web Scans and to use Google reCaptcha for Drop-Off

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 *;  
}
```

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.)

## Specify CSP to Pass Security Web Scans and to use Google reCaptcha for Drop-Off



GlobalSCAPE Knowledge Base

<https://kb.globalscape.com/Knowledgebase/11435/Specify-CSP-to-Pass-Security...>