HTTP response headers

Last Modified on 01/07/2025 2:42 pm EST

In order to improve the security of your knowledge base, you can enable some additional HTTP response headers and/or Content Security Policies that will be returned by our servers that give additional instructions to the reader's browser.

The effects of these headers vary. They should only be used by someone with a clear understanding of what they do. Consult your security team before using any of these settings.

To access these headers, go to **Security and access > Security settings**. The **HTTP response headers** section is about halfway down the page.

Here are more details on the options:

Response headers

Response headers allow us to pass additional information to your browser client.

HTTP Strict Transport Security (HSTS)

The HTTP Strict Transport Security header informs the browser that it should never load a site using HTTP and should automatically convert all attempts to access the site using HTTP to HTTPS requests instead. Refer to MDN Web Docs for more info.

X-XSS-Protection: 1

The X-XSS-Protection: 1 header enables XSS filtering (usually the default in browsers). If a cross-site scripting attack is detected, the browser will sanitize the page (remove the unsafe parts). Refer to MDN Web Docs for more info.

X-Content-Type-Options: nosniff

The X-Content-Type-Options response HTTP header is a marker used by the server to indicate that the MIME types advertised in the Content-Type headers should not be changed and should be followed. This is a way to opt out of MIME type sniffing, or, in other words, to say that the MIME types are deliberately configured. Refer to MDN Web Docs for more info.

X-Frame-Options: SAMEORIGIN/DENY

The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed

to render a page in an `<iframe>`, `<embed>`, or `<object>`. Sites can use this to avoid click-jacking attacks, by ensuring that their content is not embedded into other sites. Refer to MDN Web Docs for more info.

Content Security Policies

Content Security Policies (CSP) are 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. If you're pulling external resources, the CSP determines which domains are allowed to do certain things, such as run scripts, load resources, and so on. Refer to MDN Web Docs for more info.

You can include domains with and without the scheme (such as https:, wss:, etc.), 'unsafe-eval', and domains with wildcards (*) for any of the CSP directives here.

Proceed with caution
These options have the most potential to cause unintended consequences for your knowledge base. If you are referencing any remote JavaScript, fonts, images/files, or CSS, make sure you add the remote domains into this policy or they'll be blocked.

Defining the script-src or default-src policy may also prevent the KnowledgeOwl Modern Widget from rendering (Widget 2.0 will not be affected).

To enable CSP

We recommend that you:

1. First, review the individual directives below and add appropriate domains/settings to individual CSP directives (such as default-src, script-src, etc.). Refer to the sections below for more information on each directive.
2. Once you've reviewed all directives and added appropriate domains and resources, check the box to **Enable content security policy headers**.
3. A modal appears to confirm that you're sure you want to proceed. You must select **Enable** to proceed.
4. CSPs won't be fully enabled until you **Save**.
5. We recommend navigating around your knowledge base after you've enabled the CSP to ensure that you didn't overlook any necessary domains or resources. Console errors can help you identify things you missed!

default-src

This CSP directive is used as a fallback when any of the others don't have values specified. Refer to MDN Web Docs for more information.

We include default-src ***.knowledgeowl.com**, **'self'**, **'unsafe-inline'**, and a few other required resources here even if you don't specify them.

script-src

This CSP directive specifies valid sources for JavaScript. This includes not only URLs loaded directly into `<script>` elements, but also things like inline script event handlers like `onclick`. Refer to MDN Web Docs for more information.

Fancy Box
If you're using the Fancy Box plugin for images, include **cdnjs.cloudflare.com** in this list. You may also want to add **'unsafe-eval'** to this list. See MDN Web Docs for more information.

Before you enable, consider checking these places for domains you may be running scripts from and be sure you've added them to this directive:

- **Customize > Style (HTML & CSS) > Customize HTML, CSS, and JS > Custom HTML:** Body, Article, etc.
- **Customize > Style (HTML & CSS) > Customize HTML, CSS, and JS > Custom Head**
- **Snippets:** Check individual snippets that may be running scripts.

style-src

This CSP directive specifies valid sources for stylesheets. Refer to MDN Web Docs for more information.

Fancy Box
If you're using the Fancy Box plugin for images, include **cdnjs.cloudflare.com** in this list.

Before you enable, consider checking these places for references to external stylesheets and be sure you've added them to this directive:

- **Customize > Style (HTML & CSS) > Customize HTML, CSS, and JS > Custom HTML:** Body, Article, etc.
- **Customize > Style (HTML & CSS) > Custom Head**
- **Snippets:** Check individual snippets that may be running scripts.

font-src

This CSP directive specifies valid sources for fonts loaded using `@font-face`. Refer to MDN Web Docs for more information.

Before you enable, consider checking these places for references to font-face rules containing external resources:

- **Customize > Style (HTML & CSS) > Fonts:** If a Custom Font is selected, be sure to add that domain.
- **Customize > Style (HTML & CSS) > Customize HTML, CSS, and JS > Custom CSS:** Look for any font-face rules.
- **Customize > Style (HTML & CSS) > Customize HTML, CSS, and JS > Custom Head:** Look for any font references outside of KnowledgeOwl.
- **Snippets:** Check individual snippets to be sure they don't have font-face rules.

img-src

This CSP directive specifies valid sources for images and favicons. See MDN Web Docs for more information.

Before you enable, consider checking these places for references to images outside of KnowledgeOwl:

- **Customize > Style (HTML & CSS) > Customize HTML, CSS, and JS > Custom Head**
- **Customize > Style (HTML & CSS) > Customize HTML, CSS, and JS > Custom CSS**
- **Customize > Style (HTML & CSS) > Customize HTML, CSS, and JS > Custom HTML:** Body, Homepage, Article, etc.
- Individual snippets or articles containing external images in the body or in article thumbnails/banners