Cloudera Data Science Workbench

Configuring HTTP Headers for Cloudera Data Science Workbench

Date published: 2020-02-28
Date modified: 2020-12-15

CLOUDERA

Legal Notice

Contents

Configuring HTTP Headers for Cloudera Data Science Workbench

Cloudera Data Science Workbench 1.4.2 (and higher) include three properties that allow you to customize the HTTP headers accepted by Cloudera Data Science Workbench. They are available under the site administrator panel at Admin Security .

Required Role: Site Administrator

Important: Any changes to the following properties require a full restart of Cloudera Data Science Workbench. For CSD deployments, go to Cloudera Manager and restart the CDSW service. For RPM deployments, run cdsw restart on the master host.

Enable HTTP Security Headers

Provides information on HTTP security headers.

When Enable HTTP security headers is enabled, the following HTTP headers will be included in HTTP responses from servers:

- X-XSS-Protection
- X-DNS-Prefetch-Control
- X-Frame-Options
- X-Download-Options
- X-Content-Type-Options

This property is enabled by default .

Disabling this property could leave your Cloudera Data Science Workbench deployment vulnerable to clickjacking, cross-site scripting (XSS), or any other injection attacks.

Enable HTTP Strict Transport Security (HSTS)

When both TLS/SSL and this property (Enable HTTP Strict Transport Security (HSTS)) are enabled, Cloudera Data Science Workbench will inform your browser that it should never load the site using HTTP.

Note: Without TLS/SSL enabled, configuring this property will have no effect on your browser.

All attempts to access Cloudera Data Science Workbench using HTTP will automatically be converted to HTTPS.

This property is disabled by default .

If you ever need to downgrade to back to HTTP, use the following sequence of steps: First, deactivate this checkbox to disable HSTS and restart Cloudera Data Science Workbench. Then, load the Cloudera Data Science Workbench web application in each browser to clear the respective browser's HSTS setting. Finally, disable TLS/SSL across the cluster. Following this sequence should help avoid a situation where users get locked out of their accounts due to browser caching.

Cross-Origin Resource Sharing (CORS)

Most modern browsers implement the Same-Origin Policy, which restricts how a document or a script loaded from one origin can interact with a resource from another origin.

When the Enable cross-origin resource sharing property is enabled on Cloudera Data Science Workbench, web servers will include the Access-Control-Allow-Origin: * HTTP header in their HTTP responses. This gives web applications on different domains permission to access the Cloudera Data Science Workbench API through browsers.

This property is disabled by default .

When this property is disabled, web applications from different domains will not be able to programmatically communicate with the Cloudera Data Science Workbench API through browsers. In most circumstances, this property should remain disabled. If you have a website that needs to access the CDSW cluster, then enabling this property will make the cluster less secure.