Cross-origin resource sharing (CORS) *

Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources on a web page to be requested from another domain outside the domain from which the first resource was served.

To add the CORS authorization to the header using Apache or Litespeed Enterprise, add the following line within a .htaccess file:

```
Header set Access-Control-Allow-Origin "*"
```

Alternatively, you may also use the following:

```
# Permit OPTIONS, GET, POST, PUT and DELETE requests.

# Apache 2.2
<IfModule !mod_authz_core.c>
   <Limit OPTIONS GET POST PUT DELETE>
      Allow from all
   </Limit>
</IfModule>

# Apache 2.4
<IfModule mod_authz_core.c>
   <Limit OPTIONS GET POST PUT DELETE>
      Require all granted
   </Limit>
</IfModule>
```

You can also set a CORS header from a PHP script:

```
<?php
header("Access-Control-Allow-Origin: *");
```

You can confirm the CORS header is being set through the development tools of your web browser or using CURL with the following command:

```
curl -H "Origin: origin-example.com" --head "your-website.com"
```

CORS headers are supported on our web hosting plans and managed servers. On unmanaged servers, it should also be supported by default - depending on the web control panel and web server you are using (e.g., Directadmin or cPanel with Apache).

Troubleshooting

CORS headers are usually related to web development, especially if you are trying to integrate your web application with an API.

If you've already confirmed the CORS headers are being set on the server-side and you are still having difficulties, we would suggest rechecking the CORS parameters being used. It might be necessary to use different parameters to work with your code or API.

Would you prefer to stop worrying about the configuration of your operating system or web server? Get one of our web hosting plans or managed servers today! We'll take care of the technical aspects, so you can focus on growing your business.