

Enable Strict Transport Security In Apache Virtual Host for Nextcloud

Enable HTTP Strict Transport Security

While redirecting all traffic to HTTPS is good, it may not completely prevent man-in-the-middle attacks. Thus administrators are encouraged to set the HTTP Strict Transport Security header, which instructs browsers to not allow any connection to the Nextcloud instance using HTTP, and it attempts to prevent site visitors from bypassing invalid certificate warnings.

This can be achieved by setting the following settings within the Apache VirtualHost file:

```
<VirtualHost *:443>
  ServerName cloud.nextcloud.com
  <IfModule mod_headers.c>
    Header always set Strict-Transport-Security "max-age=15552000;
includeSubDomains"
  </IfModule>
</VirtualHost>
```

This example configuration will make all subdomains only accessible via HTTPS. If you have subdomains not accessible via HTTPS, remove `includeSubDomains`. Consider how this would affect integration with OnlyOffice Document Server hosted on a subdomain of the NextCloud domain, unless the subdomain is added to or included in the LetsEncrypt SSL certificate.

IMPORTANT: This requires the `mod_headers` extension in Apache.

Let's see how to enable headers module using `a2enmod`

How to Enable `mod_headers` in Apache Ubuntu Here's how to enable `mod_headers` in Apache Ubuntu / Debian.

1. Install `mod_headers` If you want to install Apache module such as `mod_headers`, you need to issue the `a2enmod` command

```
$ sudo a2enmod <module_name>
<code>
```

Open terminal and run the following command.

```
<code>
$ sudo a2enmod headers
```

2. Restart Apache web server for changes to take effect

```
$ sudo service apache2 restart
```

3. Check if `mod_headers` is working. You can easily check if `mod_headers` is enabled by running the following command

```
$ apachectl -M | headers
```

OR

```
$ apache2ctl -M | grep headers
```

If you see the following output, it means mod_headers is enabled and working.

```
$ headers_module (shared)
```

4. Disable mod_headers. If you want to disable/uninstall Apache module such as mod_headers, you need to issue the a2dismod command

```
$ sudo a2dismod <module_name>
```

To disable/uninstall mod_headers run the following command.

```
$ sudo a2dismod headers
```

Restart Apache web server to apply changes.

From: <https://www.installconfig.com/> - Install Config Wiki

Permanent link: https://www.installconfig.com/doku.php?id=enable_strict_transport_security_apache_virtual_host&rev=1687626269

Last update: 2023/06/24 17:04

