

The .htaccess Cheat Sheet · WebsiteSetup.org

Apache 2.4 correct syntax. Back up your file before every change. Add custom rules above or below the WordPress block, never inside it.

Redirects

Permanent 301 redirect from one old page to a new URL.

```
Redirect 301 /old.html https://example.com/new/
```

Temporary 302 redirect for short-lived changes like a sale.

```
Redirect 302 /promo https://example.com/offer/
```

Force every request onto HTTPS.

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

Add www to a bare domain (non-www to www).

```
RewriteCond %{HTTP_HOST} ^example\.com [NC]
RewriteRule ^(.*)$ https://www.example.com/$1 [L,R=301]
```

Drop www from the domain (www to non-www). Use one direction only.

```
RewriteCond %{HTTP_HOST} ^www\.example\.com [NC]
RewriteRule ^(.*)$ https://example.com/$1 [L,R=301]
```

Force a trailing slash on paths that are not real files.

```
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule ^(.*/)?$ /$1/ [L,R=301]
```

Rewrite Rules Basics

Core rewrite structure. Flags: [L]=last, [R=301]=redirect, [NC]=case-insensitive, [F]=forbidden.

```
RewriteEngine On
RewriteBase /
RewriteCond %{QUERY_STRING} ^id=10$
RewriteRule ^page$ /new-page [L]
```

Custom Error Pages

Serve your own 404 and 500 pages instead of the plain defaults.

```
ErrorDocument 404 /404.html
ErrorDocument 500 /500.html
```

Access Control

Block one IP while everyone else stays allowed.

```
<RequireAll>
    Require all granted
    Require not ip 203.0.113.5
</RequireAll>
```

Allow only your own IP (good for locking wp-admin).

```
Require ip 203.0.113.5
```

Password-protect a directory with HTTP Basic auth.

```
AuthType Basic
AuthName "Restricted Area"
AuthUserFile /home/user/.htpasswd
Require valid-user
```

Directory Options

Disable directory browsing so folder contents are not listed.

```
Options -Indexes
```

Set the default file loaded for a directory.

```
DirectoryIndex index.html index.php
```

MIME Types and Charset

Set UTF-8 as default and serve .js and .webp with correct types.

```
AddDefaultCharset UTF-8
AddType application/javascript .js
AddType image/webp .webp
```

Caching and GZIP

Cache static files in the browser (images 1 year, CSS and JS 1 month).

```
<IfModule mod_expires.c>
    ExpiresActive On
    ExpiresByType image/webp "access plus 1 year"
    ExpiresByType text/css "access plus 1 month"
    ExpiresByType application/javascript "access plus 1 month"
</IfModule>
```

Compress text-based responses with GZIP.

```
<IfModule mod_deflate.c>
    AddOutputFilterByType DEFLATE text/html text/css application/javascript text/plain image/svg+xml
</IfModule>
```

Tell caches to store compressed and uncompressed copies separately.

```
<IfModule mod_headers.c>
    Header append Vary Accept-Encoding
</IfModule>
```

Security Hardening

Block direct access to wp-config.php (holds your database password).

```
<Files wp-config.php>
    Require all denied
</Files>
```

Block xmlrpc.php, a common brute-force and DDoS target.

```
<Files xmlrpc.php>
    Require all denied
</Files>
```

Disable directory browsing.

```
Options -Indexes
```

Block aggressive crawlers by user-agent.

```
RewriteCond %{HTTP_USER_AGENT} (AhrefsBot|MJ12bot|SemrushBot) [NC]
RewriteRule .* - [F,L]
```

Stop other sites from hotlinking your images.

```
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^https?://(www\.)?example\.com [NC]
RewriteRule \.(jpe?g|png|gif|webp)$ - [F,NC,L]
```

Default WordPress Block

WordPress manages this for permalinks. Never edit inside the markers.

```
# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
RewriteBase /
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
</IfModule>
# END WordPress
```