

```

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

# #####
# # CROSS-ORIGIN #
# #####

# -----
# | Cross-origin images |
# -----

# Send the CORS header for images when browsers request it.
#
# https://developer.mozilla.org/en-US/docs/Web/HTML/CORS_enabled_image
# https://blog.chromium.org/2011/07/using-cross-domain-images-in-webgl-and.html

<IfModule mod_setenvif.c>
  <IfModule mod_headers.c>
    <FilesMatch "\.(bmp|curl gif|ico|jpe?g|png|svgz?|webp)$">
      SetEnvIf Origin ":" IS_CORS
      Header set Access-Control-Allow-Origin "*" env=IS_CORS
    </FilesMatch>
  </IfModule>
</IfModule>

# -----
# | Cross-origin web fonts |
# -----

# Allow cross-origin access to web fonts.

<IfModule mod_headers.c>
  <FilesMatch "\.(eot|otf|ttf|woff|woff2)$">

```

```
<FilesMatch \.(?!(?:|t|c|f|j|w|t|z|?)$) >
    Header set Access-Control-Allow-Origin "*"
</FilesMatch>
</IfModule>
```

```
# #####
# # ERRORS #
# #####

# -----
# | Error prevention |
# -----

# Disable the pattern matching based on filenames.
#
# This setting prevents Apache from returning a 404 error as the result
# of a rewrite when the directory with the same name does not exist.
#
# https://httpd.apache.org/docs/current/content-negotiation.html#multiviews
```

Options -MultiViews

```
# #####
# # INTERNET EXPLORER #
# #####

# -----
# | Document modes |
# -----

# Force Internet Explorer 8/9/10 to render pages in the highest mode
# available in the various cases when it may not.
#
# https://hsivonen.fi/doctype/#ie8
#
# (!) Starting with Internet Explorer 11, document modes are deprecated.
# If your business still relies on older web apps and services that were
# designed for older versions of Internet Explorer, you might want to
# consider enabling `Enterprise Mode` throughout your company.
#
# https://msdn.microsoft.com/en-us/library/ie/bg182625.aspx#docmode
```

```
# http://blogs.msdn.com/b/ie/archive/2014/04/02/stay-up-to-date-with-enterprise-mode-for-internet-explorer-11.aspx
```

```
<IfModule mod_headers.c>
```

```
Header set X-UA-Compatible "IE=edge"
```

```
# `mod_headers` cannot match based on the content-type, however,  
# the `X-UA-Compatible` response header should be send only for  
# HTML documents and not for the other resources.
```

```
<FilesMatch "\.
```

```
(appcache|atom|bbaw|bmp|crx|css|curl|eot|f4[abv]|flv|geojson|gif|htc|ico|jpe?  
|js|json(ld)?
```

```
|m4[av]|manifest|map|mp4|oex|og[agv]|opus|otf|pdf|png|rdf|rss|safariextz|svgz?
```

```
|swf|topojson|tt[cf]|txt|vcard|vcf|vtt|webapp|web[mp]|webmanifest|woff2?|xld|xll|xpi)$">
```

```
Header unset X-UA-Compatible
```

```
</FilesMatch>
```

```
</IfModule>
```

```
# #####  
# # MEDIA TYPES AND CHARACTER ENCODINGS #  
# #####
```

```
# -----  
# | Media types |  
# -----
```

```
# Serve resources with the proper media types (f.k.a. MIME types).
```

```
#
```

```
# https://www.iana.org/assignments/media-types/media-types.xhtml
```

```
# https://httpd.apache.org/docs/current/mod/mod\_mime.html#addtype
```

```
<IfModule mod_mime.c>
```

```
# Data interchange
```

```
AddType application/atom+xml atom
```

```
AddType application/json json map topojson
```

```
AddType application/ld+json jsonld
```

```
AddType application/rss+xml          rss
AddType application/vnd.geo+json      geojson
AddType application/xml               rdf xml
```

JavaScript

```
# Normalize to standard type.
# https://tools.ietf.org/html/rfc4329#section-7.2
```

```
AddType application/javascript       js
```

Manifest files

```
AddType application/manifest+json   webmanifest
AddType application/x-web-app-manifest+json webapp
AddType text/cache-manifest          appcache
```

Media files

```
AddType audio/mp4                   f4a f4b m4a
AddType audio/ogg                    oga ogg opus
AddType image/bmp                    bmp
AddType image/svg+xml                svg svgz
AddType image/webp                   webp
AddType video/mp4                    f4v f4p m4v mp4
AddType video/ogg                    ogv
AddType video/webm                   webm
AddType video/x-flv                  flv
```

```
# Serving `.ico` image files with a different media type
# prevents Internet Explorer from displaying them as images:
# https://github.com/h5bp/html5-
```

```
boilerplate/commit/37b5fec090d00f38de64b591bcddcb205aadf8ee
```

```
AddType image/x-icon                cur ico
```

Web fonts

```
AddType application/font-woff       woff
AddType application/font-woff2       woff2
AddType application/vnd.ms-fontobject eot
```

```
# Browsers usually ignore the font media types and simply sniff  
# the bytes to figure out the font type.  
# https://mimesniff.spec.whatwg.org/#matching-a-font-type-pattern  
#  
# However, Blink and WebKit based browsers will show a warning  
# in the console if the following font types are served with any  
# other media types.
```

```
AddType application/x-font-ttf          ttc ttf  
AddType font/opentype                   otf
```

```
# Other
```

```
AddType application/octet-stream       safariextz  
AddType application/x-bb-appworld       bbaw  
AddType application/x-chrome-extension  crx  
AddType application/x-opera-extension   oex  
AddType application/x-xpinstall         xpi  
AddType text/vcard                      vcard vcf  
AddType text/vnd.rim.location.xloc      xloc  
AddType text/vtt                        vtt  
AddType text/x-component                 htc
```

```
</IfModule>
```

```
# -----  
# | Character encodings |  
# -----
```

```
# Serve all resources labeled as `text/html` or `text/plain`  
# with the media type `charset` parameter set to `UTF-8`.  
#  
# https://httpd.apache.org/docs/current/mod/core.html#adddefaultcharset
```

```
AddDefaultCharset utf-8
```

```
# -----  
# Serve the following file types with the media type `charset`  
# parameter set to `UTF-8`.
```

```
#
# https://httpd.apache.org/docs/current/mod/mod\_mime.html #addcharset

<IfModule mod_mime.c>
    AddCharset utf-8 .atom \
        .bbaw \
        .css \
        .geojson \
        .js \
        .json \
        .jsonld \
        .manifest \
        .rdf \
        .rss \
        .topojson \
        .vtt \
        .webapp \
        .webmanifest \
        .xloc \
        .xml
</IfModule>

# #####
# # REWRITES #
# #####

# -----
# | Rewrite engine |
# -----

# (1) Turn on the rewrite engine (this is necessary in order for
#     the `RewriteRule` directives to work).
#
#     https://httpd.apache.org/docs/current/mod/mod\_rewrite.html #RewriteEngine
#
# (2) Enable the `FollowSymLinks` option if it isn't already.
#
#     https://httpd.apache.org/docs/current/mod/core.html #options
#
# (3) If your web host doesn't allow the `FollowSymLinks` option,
#     you need to comment it out or remove it, and then uncomment
```

```
#   the `Options +SymLinksIfOwnerMatch` line (4), but be aware
#   of the performance impact.
#
#   https://httpd.apache.org/docs/current/misc/perf-tuning.html#symlinks
#
# (4) Some cloud hosting services will require you set `RewriteBase`.
#
#   https://www.rackspace.com/knowledge\_center/frequently-asked-question/why-is-modrewrite-not-working-on-my-site
#   https://httpd.apache.org/docs/current/mod/mod\_rewrite.html#rewritebase
#
# (5) Depending on how your server is set up, you may also need to
#   use the `RewriteOptions` directive to enable some options for
#   the rewrite engine.
#
#   https://httpd.apache.org/docs/current/mod/mod\_rewrite.html#rewriteoptions
#
# (6) Set %(ENV:PROTO) variable, to allow rewrites to redirect with the
#   appropriate schema automatically (http or https).
```

```
<IfModule mod_rewrite.c>
```

```
    # (1)
    RewriteEngine On

    # (2)
    Options +FollowSymlinks

    # (3)
    # Options +SymLinksIfOwnerMatch

    # (4)
    # RewriteBase /

    # (5)
    # RewriteOptions <options>

    # (6)
    RewriteCond %{HTTPS} =on
    RewriteRule ^ - [env=proto:https]
    RewriteCond %{HTTPS} !=on
```

```
RewriteRule ^ - [env=proto:http]
```

```
</IfModule>
```

```
# -----  
# | Suppressing / Forcing the `www.` at the beginning of URLs |  
# -----
```

```
# The same content should never be available under two different  
# URLs, especially not with and without `www.` at the beginning.  
# This can cause SEO problems (duplicate content), and therefore,  
# you should choose one of the alternatives and redirect the other  
# one.
```

```
#  
# By default `Option 1` (no `www.`) is activated.
```

```
# http://no-www.org/faq.php?q=class_b
```

```
#  
# If you would prefer to use `Option 2`, just comment out all the  
# lines from `Option 1` and uncomment the ones from `Option 2`.
```

```
#  
# (!) NEVER USE BOTH RULES AT THE SAME TIME!
```

```
# -----
```

```
# Option 1: rewrite www.example.com + example.com
```

```
<IfModule mod_rewrite.c>
```

```
    RewriteEngine On
```

```
    RewriteCond %{HTTPS} !=on
```

```
    RewriteCond %{HTTP_HOST} ^www\.(.+)$ [NC]
```

```
    RewriteRule ^ %{ENV:PROTO}://%1%{REQUEST_URI} [R=301,L]
```

```
</IfModule>
```

```
# -----
```

```
# Option 2: rewrite example.com + www.example.com
```

```
#  
# Be aware that the following might not be a good idea if you use "real"  
# subdomains for certain parts of your website.
```

```
# <IfModule mod_rewrite.c>
```



```

# -----
# RewriteEngine On
# RewriteCond %{HTTPS} !=on
# RewriteCond %{HTTP_HOST} !^www\. [NC]
# RewriteCond %{SERVER_ADDR} !=127.0.0.1
# RewriteCond %{SERVER_ADDR} !=::1
# RewriteRule ^ %{ENV:PROTO}://www.%{HTTP_HOST}%{REQUEST_URI} [R=301,L]
# </IfModule>

# #####
# # SECURITY #
# #####

# -----
# | File access |
# -----

# Block access to directories without a default document.
#
# You should leave the following uncommented, as you shouldn't allow
# anyone to surf through every directory on your server (which may
# includes rather private places such as the CMS's directories).

<IfModule mod_autoindex.c>
    Options -Indexes
</IfModule>

# -----

# Block access to all hidden files and directories with the exception of
# the visible content from within the `/.well-known/` hidden directory.
#
# These types of files usually contain user preferences or the preserved
# state of an utility, and can include rather private places like, for
# example, the `.git` or `.svn` directories.
#
# The `/.well-known/` directory represents the standard (RFC 5785) path
# prefix for "well-known locations" (e.g.: `/.well-known/manifest.json`,
# `/.well-known/keybase.txt`), and therefore, access to its visible
# content should not be blocked.
#
# https://www.moot.net/blog/2010/04/07/well-known

```

```
# https://www.muhimbi.com/Articles/2010/04/07/Well-Known/
```

```
# https://tools.ietf.org/html/rfc5785
```

```
<IfModule mod_rewrite.c>
```

```
    RewriteEngine On
```

```
    RewriteCond %{REQUEST_URI} "!(^/)\.well-known/([^\./]+/?.?)+$" [NC]
```

```
    RewriteCond %{SCRIPT_FILENAME} -d [OR]
```

```
    RewriteCond %{SCRIPT_FILENAME} -f
```

```
    RewriteRule "(^/)\. " - [F]
```

```
</IfModule>
```

```
# -----
```

```
# Block access to files that can expose sensitive information.
```

```
#
```

```
# By default, block access to backup and source files that may be  
# left by some text editors and can pose a security risk when anyone  
# has access to them.
```

```
#
```

```
# http://feross.org/cmsploit/
```

```
#
```

```
# (!) Update the `<FilesMatch>` regular expression from below to  
# include any files that might end up on your production server and  
# can expose sensitive information about your website. These files may  
# include: configuration files, files that contain metadata about the  
# project (e.g.: project dependencies), build scripts, etc..
```

```
<FilesMatch "(^#.#|\. (bak|conf|dist|fla|in[ci]|log|psd|sh|sql|sw[op])|")$" >
```

```
# Apache < 2.3
```

```
<IfModule !mod_authz_core.c>
```

```
    Order allow,deny
```

```
    Deny from all
```

```
    Satisfy All
```

```
</IfModule>
```

```
# Apache ≥ 2.3
```

```
<IfModule mod_authz_core.c>
```

```
    Require all denied
```

```
</IfModule>
```

```
</FilesMatch>
```

```
</filesMatch>
```

```
# -----  
# | Reducing MIME type security risks |  
# -----
```

```
# Prevent some browsers from MIME-sniffing the response.
```

```
#  
# This reduces exposure to drive-by download attacks and cross-origin  
# data leaks, and should be left uncommented, especially if the server  
# is serving user-uploaded content or content that could potentially be  
# treated as executable by the browser.
```

```
#  
# http://www.slideshare.net/hasegawayosuke/owasp-hasegawa  
# http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protection.aspx  
# https://msdn.microsoft.com/en-us/library/ie/gg622941.aspx  
# https://mimesniff.spec.whatwg.org/
```

```
<IfModule mod_headers.c>
```

```
    Header set X-Content-Type-Options "nosniff"
```

```
</IfModule>
```

```
# -----  
# | Server-side technology information |  
# -----
```

```
# Remove the `X-Powered-By` response header that:
```

```
#  
# * is set by some frameworks and server-side languages  
#   (e.g.: ASP.NET, PHP), and its value contains information  
#   about them (e.g.: their name, version number)
```

```
#  
# * doesn't provide any value as far as users are concern,  
#   and in some cases, the information provided by it can  
#   be used by attackers
```

```
#  
# (!) If you can, you should disable the `X-Powered-By` header from the  
# language / framework level (e.g.: for PHP, you can do that by setting  
# `expose_php = off` in `php.ini`)
```

```
#  
"....."  
"....."
```

```
# https://php.net/manual/en/ini.core.php#ini.expose\_php
```

```
<IfModule mod_headers.c>  
    Header unset X-Powered-By  
</IfModule>
```

```
# -----  
# | Server software information |  
# -----
```

```
# Prevent Apache from adding a trailing footer line containing  
# information about the server to the server-generated documents  
# (e.g.: error messages, directory listings, etc.)  
#  
# https://httpd.apache.org/docs/current/mod/core.html#serversignature
```

```
ServerSignature Off
```

```
# #####  
# # WEB PERFORMANCE #  
# #####
```

```
# -----  
# | Compression |  
# -----
```

```
<IfModule mod_deflate.c>
```

```
    # Force compression for mangled `Accept-Encoding` request headers  
    # https://developer.yahoo.com/blogs/ydn/pushing-beyond-gzipping-25601.html
```

```
    <IfModule mod_setenvif.c>  
        <IfModule mod_headers.c>  
            SetEnvIfNoCase ^(\Accept-EncodXng|X-cept-Encoding|X(15)|^(15)|-(15))$  
            ^((gzip|deflate)\s*,?\s*)+([X"]-){4,13}$ HAVE_Accept-Encoding  
            RequestHeader append Accept-Encoding "gzip,deflate" env=HAVE_Accept-Encoding  
        </IfModule>  
    </IfModule>
```

```
# -----
```

```
# Compress all output labeled with one of the following media types.
#
# (!) For Apache versions below version 2.3.7 you don't need to
# enable `mod_filter` and can remove the ``
# and `` lines as `AddOutputFilterByType` is still in
# the core directives.
#
# https://httpd.apache.org/docs/current/mod/mod\_filter.html#addoutputfilterbytype
```

```
<IfModule mod_filter.c>
```

```
    AddOutputFilterByType DEFLATE "application/atom+xml" \
        "application/javascript" \
        "application/json" \
        "application/ld+json" \
        "application/manifest+json" \
        "application/rdf+xml" \
        "application/rss+xml" \
        "application/schema+json" \
        "application/vnd.geo+json" \
        "application/vnd.ms-fontobject" \
        "application/x-font-ttf" \
        "application/x-javascript" \
        "application/x-web-app-manifest+json" \
        "application/xhtml+xml" \
        "application/xml" \
        "font/eot" \
        "font/opentype" \
        "image/bmp" \
        "image/svg+xml" \
        "image/vnd.microsoft.icon" \
        "image/x-icon" \
        "text/cache-manifest" \
        "text/css" \
        "text/html" \
        "text/javascript" \
        "text/plain" \
        "text/vcard" \
        "text/vnd.rim.location.xloc" \
        "text/vtt" \
        "text/x-component" \
        "text/x-cross-domain-policy" \
```

```
"text/xml"
```

```
</IfModule>
```

```
# -----  
  
# Map the following filename extensions to the specified  
# encoding type in order to make Apache serve the file types  
# with the appropriate `Content-Encoding` response header  
# (do note that this will NOT make Apache compress them!).  
#  
# If these files types would be served without an appropriate  
# `Content-Enable` response header, client applications (e.g.:  
# browsers) wouldn't know that they first need to uncompress  
# the response, and thus, wouldn't be able to understand the  
# content.  
#  
# https://httpd.apache.org/docs/current/mod/mod\_mime.html#addencoding
```

```
<IfModule mod_mime.c>
```

```
    AddEncoding gzip          svgz
```

```
</IfModule>
```

```
</IfModule>
```

```
# -----  
# | ETags |  
# -----
```

```
# Remove `ETags` as resources are sent with far-future expires headers.  
#  
# https://developer.yahoo.com/performance/rules.html#etags  
# https://tools.ietf.org/html/rfc7232#section-2.3
```

```
# `FileETag None` doesn't work in all cases.
```

```
<IfModule mod_headers.c>
```

```
    Header unset ETag
```

```
</IfModule>
```

```
FileETag None
```

```

# -----
# | Expires headers |
# -----

# Serve resources with far-future expires headers.
#
# (!) If you don't control versioning with filename-based
# cache busting, you should consider lowering the cache times
# to something like one week.
#
# https://httpd.apache.org/docs/current/mod/mod_expires.html

<IfModule mod_expires.c>

    ExpiresActive on
    ExpiresDefault "access plus 1 month"

# CSS

    ExpiresByType text/css "access plus 1 year"

# Data interchange

    ExpiresByType application/atom+xml "access plus 1 hour"
    ExpiresByType application/rdf+xml "access plus 1 hour"
    ExpiresByType application/rss+xml "access plus 1 hour"

    ExpiresByType application/json "access plus 0 seconds"
    ExpiresByType application/ld+json "access plus 0 seconds"
    ExpiresByType application/schema+json "access plus 0 seconds"
    ExpiresByType application/vnd.geo+json "access plus 0 seconds"
    ExpiresByType application/xml "access plus 0 seconds"
    ExpiresByType text/xml "access plus 0 seconds"

# Favicon (cannot be renamed!) and cursor images

    ExpiresByType image/vnd.microsoft.icon "access plus 1 week"
    ExpiresByType image/x-icon "access plus 1 week"

# HTML

```

ExpiresByType text/html "access plus 0 seconds"

JavaScript

ExpiresByType application/javascript "access plus 1 year"

ExpiresByType application/x-javascript "access plus 1 year"

ExpiresByType text/javascript "access plus 1 year"

Manifest files

ExpiresByType application/manifest+json "access plus 1 week"

ExpiresByType application/x-web-app-manifest+json "access plus 0 seconds"

ExpiresByType text/cache-manifest "access plus 0 seconds"

Media files

ExpiresByType audio/ogg "access plus 1 month"

ExpiresByType image/bmp "access plus 1 month"

ExpiresByType image/gif "access plus 1 month"

ExpiresByType image/jpeg "access plus 1 month"

ExpiresByType image/png "access plus 1 month"

ExpiresByType image/svg+xml "access plus 1 month"

ExpiresByType image/webp "access plus 1 month"

ExpiresByType video/mp4 "access plus 1 month"

ExpiresByType video/ogg "access plus 1 month"

ExpiresByType video/webm "access plus 1 month"

Web fonts

Embedded OpenType (EOT)

ExpiresByType application/vnd.ms-fontobject "access plus 1 month"

ExpiresByType font/eot "access plus 1 month"

OpenType

ExpiresByType font/opentype "access plus 1 month"

TrueType

ExpiresByType application/x-font-ttf "access plus 1 month"

Web Open Font Format (WOFF) 1.0

ExpiresByType application/font-woff "access plus 1 month"


```
ExpiresByType application/x-font-woff "access plus 1 month"
ExpiresByType font/woff "access plus 1 month"

# Web Open Font Format (WOFF) 2.0
ExpiresByType application/font-woff2 "access plus 1 month"

# Other

ExpiresByType text/x-cross-domain-policy "access plus 1 week"
```

```
</IfModule>
```