Apache .htaccess for Exponential 6

DirectoryIndex index.php

Source file: doc/eng-us/examples/htaccess Last changed 2026-11-04
https://doc.exponential.earth/exphelp/viewer/examples/htaccess

```
# Apache .htaccess for Exponential 6
# ------------------------------------------------------------------------
# What this is: the rewrite rules that make Apache serve an Exponential
# installation safely when the document root is the installation root (the
# directory with index.php). Only a fixed list of asset paths is sent as a
# file; every other request (URL aliases, modules, and also settings/, var/,
# vendor/, kernel/, composer.json) is answered by index.php, which never hands
# out the file. Dot files (.git, .env, .htaccess) answer 404 anywhere, and no
# .php below the root runs because its path was asked for.
#
# How to install it: the shipped file is .htaccess_root in the installation
# root. Copy it, do not move it, so an update can bring a new version:
#
#     cp .htaccess_root .htaccess
#
# The section "Rules" below is a verbatim copy of .htaccess_root of this
# release, for reading and for copying into a <Directory> block. The section
# "Optional" after it is not in .htaccess_root: HTTPS redirect, headers on
# static files and browser caching, each switched off or guarded until you
# turn it on. Never delete a rule of the "Rules" section to make something
# work; find the cause instead (doc/eng-us/install/13-security-hardening.md, 13.2).
#
# Needs: mod_rewrite, and AllowOverride All (or at least FileInfo) for the
# directory. Check with "apachectl configtest", then these requests:
#   /.git/config, /.env, /kernel/classes/ezini.php  -> 404
#   /settings/site.ini, /composer.json               -> a page from index.php, never the file
#
# Explained rule by rule: doc/eng-us/examples/web-servers/apache-htaccess.md
# The same rules for a virtual host (server context): doc/eng-us/examples/ezpublish.conf
#
# License: the first versions of this file came with the software Exponential
# grew out of, eZ Publish, 1999 - 2014. The rewrite rules are those of
# .htaccess_root, part of the software (GNU General Public License version 2
# or later, like the rest of the code). This documented example, its comments
# and optional sections, is free documentation under the GNU Free
# Documentation License 1.3 or later (doc/eng-us/README-LICENSE.md).

# ========================================================================
# Rules (verbatim .htaccess_root)
# ========================================================================

# Copy this file to a new file called .htaccess in your Exponential root
# to secure your installation by turning on .htaccess based virtual host mode.

DirectoryIndex index.php

RewriteEngine On
# No dot file or dot directory (.git, .env, .htaccess ...) is served or
# run, whatever folder it lies in; .well-known stays reachable.
RewriteRule (^|/)\.(?!well-known(/|$)) - [R=404,L]
# No script runs because its path was asked for, except the front
```

```
# controllers at the root: a .php below them (in the package store,
# an extension, var/) answers 404 instead of being executed.
RewriteCond %{REQUEST_FILENAME} -f
RewriteRule ^.+/[^/]+\.(php[0-9]?|phtml|phar)$ - [R=404,L]
RewriteRule ^api/ index_rest.php [L]
RewriteRule ^index_rest\.php - [L]
# The SOAP server (settings/soap.ini EnableSOAP=true) is index_soap.php since
# Exponential 6.0.15; soap.php, its old name, only forwards to it. Uncomment
# when SOAP is switched on, and let the SOAP clients call index_soap.php:
#RewriteRule ^index_soap\.php - [L]
RewriteRule ^([^/]+/)?content/treemenu.* index_treemenu.php [L]
# WebDAV (settings/webdav.ini [GeneralSettings] EnableWebDAV=true): the server is
# index_webdav.php, reached as https://www.example.com/index_webdav.php/<siteaccess>/.
# Uncomment to let it answer on this host, or give it a host of its own that sends
# every request to index_webdav.php. webdav.php, its old name, only forwards to it
# and will be removed in a later major version: name index_webdav.php in new rules.
#RewriteRule ^index_webdav\.php - [L]
RewriteRule ^var/([^/]+/)?storage/images(-versioned)?/.* - [L]
# SVG images are sanitized on upload; served from the storage they also run
# nothing and load nothing when opened directly (needs mod_headers).
<IfModule mod_headers.c>
    <FilesMatch "(?i)\.svgz?$">
        Header always set Content-Security-Policy "sandbox; default-src 'none'; style-src 'uns
afe-inline'"
        Header always set X-Content-Type-Options "nosniff"
    </FilesMatch>
</IfModule>
# The stored files of PDF exports generated once (Setup > PDF export): only
# names of letters, digits, ".", "_" and "-" ending in .pdf, as the export writes them.
RewriteRule ^var/([^/]+/)?storage/pdf/[A-Za-z0-9][A-Za-z0-9._-]*\.pdf$ - [L]
# Of the originals only the images (SVG images are shown from there);
# other uploads stay behind content/download and its permissions.
RewriteRule ^var/([^/]+/)?storage/original/image/.+\.(png|jpe?g|gif|webp|svg)$ - [L]
RewriteRule ^var/([^/]+/)?cache/(texttoimage|public)/.* - [L]
# With site.ini [FileSettings] CacheVarDir=var_cache (the caches of the sites in a
# tree of their own, multi-site hosting) their public caches are served from there:
#RewriteRule ^var_cache/([^/]+/)?cache/(texttoimage|public)/.* - [L]
RewriteRule ^design/[^/]+/(stylesheets|images|javascript|fonts)/.* - [L]
RewriteRule ^share/icons/.* - [L]
# Icon themes shipped by extensions (icon.ini [ExtensionSettings] IconExtensions[],
# extension/<name>/icons/). Only images with exactly one extension: a name like
# a.php.svg could otherwise be handed to PHP by an AddHandler mapping.
RewriteRule ^extension/[^/]+/icons/[A-Za-z0-9_/-]+\.(svg|png|gif)$ - [L]
RewriteRule ^extension/[^/]+/design/[^/]+/(stylesheets|flash|images|lib|javascripts?|fonts|ven
dor|media)/.* - [L]
RewriteRule ^packages/styles/.+/(stylesheets|images|javascript)/[^/]+/.* - [L]
RewriteRule ^packages/styles/.+/thumbnail/.* - [L]
# Only the preview images of imported packages: their XML, SQL and
# settings are not for the web.
RewriteRule ^var/storage/packages/.+\.(png|jpe?g|gif|webp)$ - [L]

#  Makes it possible to placed your favicon at the root of your
#  Exponential instance. It will then be served directly.
RewriteRule ^favicon\.ico - [L]
#  Uncomment the line below if you want you favicon be served from the standard design.
#  You can customize the path to favicon.ico by replacing design/standard/images/favicon.ico
#  by the adequate path.
#RewriteRule ^favicon\.ico /design/standard/images/favicon.ico [L]
RewriteRule ^design/standard/images/favicon\.ico - [L]
```

```
# Give direct access to robots.txt for use by crawlers (Google, Bing, Spammers..)
RewriteRule ^robots\.txt - [L]

# The site's service workers, which have to be served from the root: index.js, the
# Exponential Service Workers Index, and sw.js, its old name, kept for browsers registered bef
ore.
RewriteRule ^index\.js$ - [L]
RewriteRule ^sw\.js$ - [L]

# Uncomment the following lines when using popup style debug.
# RewriteRule ^var/cache/debug\.html.* - [L]
# RewriteRule ^var/[^/]+/cache/debug\.html.* - [L]

# Platform for Privacy Preferences Project ( P3P ) related files for Internet Explorer
# More info here : http://en.wikipedia.org/wiki/P3p
RewriteRule ^w3c/p3p\.xml - [L]

## >>> LiteSpeed page cache (off) >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
## LiteSpeed Web Server (Enterprise) and OpenLiteSpeed can keep whole pages and
## answer anonymous visitors and crawlers from them without running PHP: no
## plugin and no code, only the rules below. Apache and nginx never read them
## (<IfModule LiteSpeed>). Every line, purging, checks and troubleshooting:
##   doc/eng-us/guides/litespeed-page-cache.md
##
## To switch it on, remove the first "#" of every line from the ">>>" line to
## the "<<<" line (a "##" line keeps one "#" and stays a comment), or run:
##   sed -i '/^## >>> LiteSpeed page cache/,/^## <<< LiteSpeed page cache/ s/^#//' .htaccess
## Then request a page twice without cookies; the second answer says "hit":
##   curl -sI https://www.example.com/ | grep -i x-litespeed-cache
## The server needs a cache directory (LiteSpeed Enterprise: CacheRoot at
## server level). OpenLiteSpeed reads only the rewrite rules of .htaccess,
## only with autoLoadHtaccess on and only after a restart, and needs its cache
## module on for the virtual host: see the guide.
##
#<IfModule LiteSpeed>
## Look the request up in the page cache.
#CacheLookup on
## Only reads: every form (POST) and every other write reaches PHP.
#RewriteCond %{REQUEST_METHOD} ^(GET|HEAD)$
## No query string: searches, filters and tracking parameters reach PHP.
#RewriteCond %{QUERY_STRING} ^$
## Nobody with a session or signed in. The session cookie is PHPSESSID with
## site.ini [Session] SessionNameHandler=default (php.ini session.name) and
## eZSESSID<md5 of the siteaccess> with SessionNameHandler=custom; the kernel
## sets is_logged_in=true for every signed-in user. Editors, members and a
## visitor with a basket all carry one. Add cookies of your own that change
## what a page shows, separated by "|".
#RewriteCond %{HTTP_COOKIE} !(eZSESSID|PHPSESSID|is_logged_in) [NC]
## Not the views that differ per visitor or change something, with or without
## a siteaccess in front: the administration (put the URI of yours if it is
## not "admin"), user/, shop/, notification/, layout/, ezjscore/, setup/ and
## every content/ view except content/view/. REST, SOAP, WebDAV and the tree
## menu never get here: the rules above send them their own way.
#RewriteCond %{REQUEST_URI} !^/([^/]+/)?((admin|user|shop|notification|layout|ezjscore|setup)(
/|$)|content/(?!view/)) [NC]
## The administration on a host name of its own: remove one more "#", adjust.
##RewriteCond %{HTTP_HOST} !^admin\. [NC]
## Keep the page 120 seconds (max-age). Nothing removes it when an editor
## publishes: anonymous visitors see a change at most max-age seconds later.
## Never cache pages with debug output (site.ini DebugOutput, DebugByIP).
```

```
#RewriteRule .* - [E=cache-control:max-age=120]
#</IfModule>
## <<< LiteSpeed page cache <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

RewriteRule .* index.php

# ============================================================================
# Optional (not in .htaccess_root). Read each block before enabling it.
# ============================================================================
#
# Nothing below changes which paths are served or routed. Blocks 2 and 3 only
# add response headers; block 1 is a redirect and is the only one that must
# move (see its comment). mod_headers needs AllowOverride FileInfo, mod_expires
# AllowOverride Indexes; without them Apache answers 500.

# --- 1. Redirect plain HTTP to HTTPS ----------------------------------------
# Off by default. Better done in the port 80 virtual host
# (doc/eng-us/examples/ezpublish.conf). If you can only use .htaccess, move these two
# lines directly below "RewriteEngine On" above and remove the "#".
# Behind a proxy or load balancer that terminates TLS, %{HTTPS} is always
# "off" here: test X-Forwarded-Proto instead, and only if the proxy always
# sets it (else every request loops):
#   RewriteCond %{HTTP:X-Forwarded-Proto} !https
#RewriteCond %{HTTPS} off
#RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]

# --- 2. Security headers on static files ------------------------------------
# The kernel sends these on its own pages (site.ini [HTTPHeaderSettings]
# SecurityHeaders[]); Apache sends nothing extra on files it serves itself.
# These are the same values as the kernel's defaults. "setifempty" keeps a
# header that index.php already sent.
<IfModule mod_headers.c>
    Header setifempty X-Content-Type-Options "nosniff"
    Header setifempty X-Frame-Options "SAMEORIGIN"
    Header setifempty Referrer-Policy "strict-origin-when-cross-origin"
    Header setifempty Permissions-Policy "camera=(), microphone=(), payment=(), usb=()"
    # HSTS: only once every name of the site is served over HTTPS for good.
    # Start short (300) and raise it to a year later; a browser remembers it
    # for the whole period (doc/eng-us/install/13-security-hardening.md, 13.9).
    # Set it here or in site.ini SecurityHeaders[Strict-Transport-Security],
    # not in both places.
    #Header always set Strict-Transport-Security "max-age=300" "expr=%{HTTPS} == 'on'"
</IfModule>

# --- 3. Browser caching of images and design files --------------------------
# Image URLs change when the image changes (the version is in the path), so
# they can be cached for a long time. Design files keep their names: keep
# their lifetime short, or use the packer's file names with the modification
# time (ezjscore.ini [Packer] AppendLastModifiedTime=enabled).
<IfModule mod_expires.c>
    <If "%{REQUEST_URI} =~ m#^/var/([^/]+/)?storage/images(-versioned)?/#">
        ExpiresActive On
        ExpiresDefault "access plus 1 year"
    </If>
    <ElseIf "%{REQUEST_URI} =~ m#^/(extension/[^/]+/)?design/[^/]+/(stylesheets|images|javascr
ipts?|fonts|lib)/#">
        ExpiresActive On
        ExpiresDefault "access plus 7 days"
    </ElseIf>
    <ElseIf "%{REQUEST_URI} =~ m#^/(share|extension/[^/]+)/icons/#">
```

```
        ExpiresActive On
        ExpiresDefault "access plus 7 days"
    </ElseIf>
</IfModule>
```

Exponential Copyright © 1998-2026 Exponential Foundation and 7x
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".
This documentation is free documentation, licensed under the GNU Free Documentation License 1.3 or later:
https://www.gnu.org/licenses/fdl-1.3.html.