

# htaccess

The .htaccess-file is mainly separated in two parts

1. some php/apache-settings
2. rewrite rules for [SEFURLs](#)

The second part, the search engine friendly URLs and rewrite rules, are described in [Rewrite Rules](#). See there for more information.

## To activate

Tiki bundles a file named `_htaccess`. You should **copy** it to `.htaccess`

Alternatively, on Linux, you can make a symlink.

```
ln -s _htaccess .htaccess
```

## PHP Settings

In some cases it is possible to overwrite some values from the [php.ini](#) file given by your ISP, by means of a file [php.ini](#) in the tiki root folder, or by means of some changes in the .htaccess file in the tiki root folder also. In this second case, place your special .htaccess file in the tiki root directory or just rename the `_htaccess` file given by Tiki to `.htaccess` and make your changes. You can visit [tiki-phpinfo.php](#) to check whether or not your changes were successful.

### PHP Version

One of the critical settings is the PHP version that should correspond to the Tiki version you are using. (see [https://doc.tiki.org/Requirements#PHP\\_](https://doc.tiki.org/Requirements#PHP_)). It is possible in some case to have several PHP versions installed on your host/server and you may need to set a different one than the default version used. You can change the value for a specific Tiki in the .htaccess file:

**Values in .htaccess by default**

```
# Option 2: PHP7 #AddType application/x-httpd-php7 .php #AddHandler application/x-httpd-php7 .php
```

Some shared host may use a different setup and require a different path for the PHP version you need. Please check with your server Admin or the company that manages it.

**Example of specific shared host value**

```
AddType x-httpd-php72 .php
```

### PHP Memory Limit

Another important setting is the php memory limit. The maximum amount of memory a script may consume. On many shared hosts this variable is set to 64MB. Tiki runs fine with 64MB but depending on your special needs and options it is necessary to uncomment and increase this value to 128MB. (which is the default value on recent PHP versions)

```
# memory limit php_value memory_limit 256M
```

## Error Display

To display php errors on your display activate / uncomment this setting. Error output is very useful during development, but it could be very dangerous in production environments. Depending on the code which is triggering the error, sensitive information could potentially leak out of your application such as database usernames and passwords or worse.

```
# to activate the error display, uncomment the following line php_flag display_errors on # to set the error reporting level,
uncomment the following line. Values are explained here: http://www.php.net/manual/en/errorfunc.constants.php php_value
error_reporting E_ALL
```

## Execution Time

PHP uses a default script execution time of 30s before a script is terminated by the server. In some cases with huge wiki pages with many plugins it's necessary to increase the execution time to 90s

```
# increase execution time (default value in php use to be 30, and in some cases of long wiki pages with many plugins it may
take longer) php_value max_execution_time = 90 ; Maximum execution time of each script, in seconds php_value
max_input_time = 90 ; Maximum amount of time each script may spend parsing request data
```

## Maximum File and Post Size

The maximum allowed size for uploaded files and maximum size of POST data that PHP will accept.

```
# increase the maximum file size for uploads allowed by php for Tiki (default value in apache use to be 2M which is usually
too low for pdf or documents with some images, screenshots, etc) php_value upload_max_filesize 10M php_value
post_max_size 11M
```

## Include Path

```
# In some cases you may see open_basedir warnings about Smarty accessing php files that it shouldn't # The following line
(uncommented) will reset the include path to use only Tiki's files which will solve this in most cases php_value include_path ""
```

Also see [latest default htaccess from code base](#)

## .htaccess content for 24.x

```
# $Id$ [This line is used to check that this configuration file is up # to date. Do not edit this line and leave it as the first line.]
# # These are suggested configuration directives for use with Tiki. # They enhance security and permit clean URLs. # In your
Tiki instance, visit tiki-admin.php?page=sefurl to make Tiki use clean URLs in generated links. # # The .htaccess file may be
enabled in number of different ways (in order of the most to the least recommended): # Option 1: Let the installer handle it. #
Option 2: Create a symbolic link from .htaccess to _htaccess. This will keep the configuration up-to-date. # Option 3: Copy
_htaccess to .htaccess. Note : Do not move (rename) _htaccess, it is required (used internally) by some Tiki features (like
SEFURL). # Option 4: Add the content of this file to your httpd.conf. # The last two options should be repeated when the
reference _htaccess file changes (when upgrading Tiki). # # DEVELOPERS: This configuration must be kept synchronized
with the configuration for other Web servers. # See
http://dev.tiki.org/Operating+System+independence#Keep_web.config_and_.htaccess_synchronized # -- Prevent Browsing of
Certain File Extensions -- # <FilesMatch "\.(bak|inc|lib|sh|tpl|sql|shtml|asp|xml|.dist)$"> <IfModule mod_authz_core.c>
Require all denied </IfModule> <IfModule !mod_authz_core.c> order deny,allow deny from all </IfModule> </FilesMatch> #
```

```
-- Prevent Browsing of Certain File Names -- # <FilesMatch
"(changelog.txt|_htaccess|README|INSTALL|web_config|copyright|.txt|composer\..*)$" > <IfModule mod_authz_core.c>
Require all denied </IfModule> <IfModule !mod_authz_core.c> order deny,allow deny from all </IfModule> </FilesMatch>
<IfModule mod_dir.c> # -- Home Page Feature -- # # Option 1: (recommended) Not using home page feature. DirectoryIndex
index.php # Option 2: If using home page feature you may avoid the home page name being appended to the url by using this
option. #DirectoryIndex tiki-index.php index.php </IfModule> # -- Ensure Caching Proxy Sends Content to Correct Client -- #
# In some distributions of Apache (e.g. Wampserver 2.5) you may also need to enable mod_filter as well for this to work.
#<IfModule mod_filter.c> <IfModule mod_deflate.c> <IfModule mod_headers.c> # Make sure proxies don't deliver the
wrong content. Header append Vary User-Agent env=!dont-vary </IfModule> AddOutputFilterByType DEFLATE text/css
text/x-component application/x-javascript application/javascript text/javascript text/x-js text/html text/richtext image/svg+xml
text/plain text/xsd text/xsl text/xml image/x-icon application/json <IfModule mod_mime.c> # DEFLATE by extension.
AddOutputFilter DEFLATE js css htm html xml svg </IfModule> </IfModule> #</IfModule> # -- Client Cache Method -- # #
Google wants either Last-Modified or ETag. Using ETags will improve the YSlow scores. # Option 1: recommended FileETag
none <IfModule mod_headers.c> # -- httpoxy mitigation -- # RequestHeader unset Proxy early # Option 2: #Header unset
ETag # -- Client Cache Expiration -- # # Google suggests to use Expires in favour of Cache-Control. # Option 1:
(recommended) Header unset Cache-Control #Option 2: #Header unset Expires # -- Persistent Connections -- # # Allow
multiple requests to be sent over the same TCP connection. Enable if you serve a lot of static content # but, be aware of the
possible disadvantages! # Read more: http://httpd.apache.org/docs/current/en/mod/core.html#keepalive #Header set
Connection Keep-Alive # -- CORS-enabled Images (@crossorigin) -- # Send CORS headers if browsers request them; enabled
by default for images. # Read more: developer.mozilla.org/en/CORS_Enabled_Image # Read more:
blog.chromium.org/2011/07/using-cross-domain-images-in-webgl-and.html # Read more: hacks.mozilla.org/2011/11/using-
cors-to-load-webgl-textures-from-cross-domain-images/ # Read more: wiki.mozilla.org/Security/Reviews/crossoriginAttribute
<IfModule mod_setenvif.c> # Mod_headers, y u no match by Content-Type?! <FilesMatch "(?i)\.(gif|png|jpe?g|svgz?|ico)$">
SetEnvIf Origin ":" IS_CORS Header set Access-Control-Allow-Origin "*" env=IS_CORS </FilesMatch> </IfModule> # --
Webfont Access -- # # Allow access from all domains for webfonts. # Alternatively you could whitelist your subdomains like
"subdomain.example.com". <FilesMatch "(?i)\.(ttf|ttc|otf|eot|woff2?)$" > Header set Access-Control-Allow-Origin "*"
</FilesMatch> # -- Enable video/audio seek -- # Header set Accept-Ranges bytes </IfModule> # -- Expires Headers -- # # If
the site is in active development, you may want to comment out this section. <IfModule mod_expires.c> <FilesMatch
"(?i)\.(gif|png|jpe?g|svgz?|ico)$"> ExpiresActive on ExpiresDefault "access plus 1 month" </FilesMatch> <FilesMatch
"(?i)\.(js|css)$"> ExpiresActive on ExpiresDefault "access plus 1 month" </FilesMatch> </IfModule> <IfModule
mod_rewrite.c> # More information: http://doc.tiki.org/Rewrite+Rules RewriteEngine On # -- Tiki Root -- # # You need to
customize the RewriteBase value below if Tiki is installed in a subdirectory of your web root. # The value needs to match the
subdirectory name that Tiki is installed in. # You will get errors otherwise. e.g. "The requested URL /absolutepath/tiki-
index.php was not found on this server" #RewriteBase /tiki # -- Redirect Missing Directories To Homepage -- # # Prevent
broken pages and slow upload times. e.g., try yourdomain.com/bogus/ or yourdomain.com/tiki/bogus/ # The below may not
work in all configurations depending on redirects already in place. # If directories containing other programs are legitimate
(e.g. when Tiki is installed in a subdirectory), then modify and enable the following line. #RewriteCond %{REQUEST_URI}
!(^/otherokaydirectory/) # If Tiki is installed in the web root and your home page is named HomePage, then enable this.
#RewriteRule ^(.+[^/])$ /HomePage [R=301,L] # If Tiki is installed in a subdirectory of the web root, then customize and
enable it below. #RewriteRule ^(.+[^/])$ /tiki/HomePage [R=301,L] # -- Legacy Template Image Locations -- # # Since
Tiki9, image locations have changed. If your custom template links to these images enabling these # options may fix your
broken images. # The preferred solution is to change the directory paths in your custom template. # Read more:
http://dev.tiki.org/ImgDirectoryRevamp #RewriteRule ^img/icons2/(.*)$ img/icons/$1 #RewriteRule ^pics/large/(.*)$
img/icons/large/$1 #RewriteRule ^img/mytiki/(.*)$ img/icons/large/$1 #RewriteRule ^pics/(.*)$ img/$1 #RewriteRule
^images/(.*)$ img/icons/$1 # Redirect drawio requests to the correct path RewriteRule ^img/lib/(.*)$
vendor/tikiwiki/diagram/img/lib/$1 [NC,L] # -- Apache Authorization Header -- # # Rewrite rules for passing authorization
with Apache running in CGI or FastCGI mode RewriteCond %{HTTP:Authorization} ^(.*) RewriteRule ^(.*) -
[E=HTTP_AUTHORIZATION:%1] # -- Prevent HTTP TRACE method -- # RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F] # -- Disallow access to hidden files (apart from well-known ones) -- # RewriteRule "(^/)\.(?!well-known)" -
[F,L] # Redirect robots.txt to dynamic tiki-robots.php file. RewriteRule ^robots\.txt$ route.php [L] # -- If the URL Points to a
File Then do Nothing -- # RewriteCond %{REQUEST_FILENAME} -s [OR] RewriteCond %{REQUEST_FILENAME} -l [OR]
RewriteCond %{REQUEST_FILENAME} -f [OR] RewriteCond %{REQUEST_FILENAME} -d RewriteRule (.*) - [L] # --
CalDAV/CardDAV service auto-discovery -- # RewriteRule ^.well-known/caldav$ tiki-caldav.php [R=301,L] RewriteRule
^.well-known/carddav$ tiki-carddav.php [R=301,L] # -- Profiles Repository -- # # Set the parentId (here set as 1) to the Id of
the category containing your profile pages. # Enable feature_wiki_export, feature_wiki and feature_categories in your Tiki
settings. # Enable tiki_p_view_category and tiki_p_export_wiki in Tiki for anonymous to be a repository. # Read more:
http://doc.tiki.org/Profiles #RewriteRule ^profiles$ tiki-
browse_categories.php?find=&deep=on&type=wiki+page&parentId=1&sort_mode=name_asc&plain&maxRecords=100000
[L] # -- Plain Text Sitemap SEO -- # # Makes a short link to a list of objects to export as a plain text sitemap. # Set the
parentId (here set as 2) to the id of a category containing the objects you wish to be # crawled by search engines.
#RewriteRule ^sitemap.txt$ tiki-
browse_categories.php?find=&deep=on&type=wiki+page&parentId=2&sort_mode=name_asc&links&maxRecords=100000
[L] # -- RSS Feeds -- # # Example rewrite rule to use the search as a simple RSS feed #RewriteRule feed-(.*)\.rss tiki-
searchindex.php?httpaccept=application%2Frss%2Bxml&filter~content=$1 [QSA,L] # If you use session_protected and
want to use apache monitoring you may get "certificate verify failed" errors on https://127.0.0.1/server-status # If so,
```

```

uncomment this line which will route these requests straight to apache and so not get forced into https # RewriteRule
^server-status.* - [L] # -- Tiki URL Rewriting -- # # Read more: https://dev.tiki.org/URL+Rewriting+Revamp RewriteRule .*
route.php [L] # -- Tiki Username Link -- # # Option 1: Exact Match. # Access a link to any user by providing its username e.g
www.yourtiki.me/u:myusername. # RewriteRule ^u:([A-Za-z0-9]+) tiki-view_tracker_item.php?user=$1&view=+user [QSA,L]
# Option 2: String Match. # Adapt with your user tracker id and user selector field id # RewriteRule ^u:([A-Za-z0-9]+) tiki-
view_tracker.php?trackerId=1&filterfield=3&filtervalue{[3]}=$1 [QSA,L] </IfModule> # -- Prevent Directory Browsing -- # #
Some shared hosting environments block options, so first check if the module is enabled <IfModule !mod_dir> Options -
Indexes </IfModule> # -- Developer cTag Blocking -- # # This prevents reading of tags file for developers who run ctags on
their server. #<Files tags> # <IfModule mod_authz_core.c> # Require all denied # </IfModule> # <IfModule
!mod_authz_core.c> # order deny,allow # deny from all # </IfModule> # </Files> # -- Web Server Auth -- # # Option 1:
recommended #AuthType Basic #AuthName "Restricted Access" #AuthUserFile /etc/httpd/passwords #Require valid-user #
Option 2: Allows services that POST back to Tiki, but less secure. #<Limit GET> # Require valid-user #</Limit> # -- Apache
Error Handling -- # # Tiki can catch some errors and deal with them by redirecting to a similar page, sending you to the #
search, etc. However, some errors do not reach Tiki and are only caught by Apache (ex.: filenameThatDoesntExist.php). # To
make Tiki handle errors caught by Apache, uncomment some of the following lines and adapt the page names. # You must
create the pages before trying to use them. #ErrorDocument 404 /tiki-index.php?page=File+not+found #ErrorDocument 500
/tiki-index.php?page=Server+error # -- Permanent Redirects -- # # This is useful if you were using another Web application
or static HTML and you want to avoid broken links. #Redirect 301 /oldpage.html /tiki-index.php?page=newpage # -- Force
PHP Version -- # # Tiki requires PHP5.6 - PHP7. If your host doesn't run one of these by default, it's possible that it can # be
activated by trying to enable it here. Check with your host. # Option 1: PHP5 #AddType application/x-httpd-php5 .php
#AddHandler application/x-httpd-php5 .php # Option 2: PHP7 #AddType application/x-httpd-php7 .php #AddHandler
application/x-httpd-php7 .php # -- Pass User/Object Information to Server Logs -- # #SetEnv TIKI_HEADER_REPORT_ID
tikiwiki #SetEnv TIKI_HEADER_REPORT_USER on #SetEnv TIKI_HEADER_REPORT_OBJECT on #SetEnv
TIKI_HEADER_REPORT_EVENTS on # -- PHP Settings -- # # If possible, it's better to change the following settings through
your php.ini file, or through your webhosting control panel. # Some web hosts will not allow you to change these setting
through the .htaccess file. # If you are not using PHP as an apache module, the following PHP settings will likely have no
effect. # For instance, if you use PHP-FPM, you will need to create a file named .user.ini and the syntax is a little different. #
For instance, a sample line would be "memory_limit=256M" (without the quotes) # To activate the error display, uncomment
the following line. # Read more http://php.net/manual/en/errorfunc.configuration.php#ini.display-errors #php_flag
display_errors on # To set the error_reporting level, uncomment the following line. # Read more:
http://php.net/manual/en/errorfunc.configuration.php#ini.error-reporting #php_value error_reporting E_ALL # Increase
memory limit (default is 128M). Use this if you are getting blank pages and/or strange errors. # Read more:
http://php.net/manual/en/ini.core.php#ini.memory-limit #php_value memory_limit 256M # Increase execution time. # Default
value in Apache used to be 30, and in some cases of long wiki pages with many plugins it may take longer. # Read more:
http://php.net/manual/en/info.configuration.php#ini.max-execution-time #php_value max_execution_time 90 # This sets the
maximum time in seconds a script is allowed to parse input data, like POST and GET. #php_value max_input_time 90 #
Increase the maximum file size for uploads allowed by PHP. # Default value in Apache used to be 2M which is usually too low
for PDF or documents with some images, screenshots, etc. # Read more:
http://php.net/manual/en/ini.core.php#ini.upload-max-filesize # Read more:
http://php.net/manual/en/ini.core.php#ini.post-max-size #php_value upload_max_filesize 10M #php_value post_max_size 11M
# In some cases you may see open_basedir warnings about Smarty accessing PHP files that it shouldn't. # The following line
(uncommented) will reset the include path to use only Tiki's files which will solve this in most cases. #php_value include_path
"." # Set a character set #php_value default_charset utf-8 # Timezone # Needed for dates and times to work properly in PHP.
# Option 1: recommended #php_value date.timezone "America/New York" # Option 2: Set the apache environment variable
#SetEnv TZ America/New York # If the packages control panel is picking up the wrong version of php (as seen in the
"diagnose" tab) # it might be because the apache PATH directive is set wrongly, so try something like this: #SetEnv PATH
/opt/local/bin:/opt/local/sbin:/usr/local/bin:/usr/bin:/bin:/usr/sbin:/sbin

```

## Related Links

- [Check](#)
- [Search engine optimization](#)
- [Rewrite Rules](#)
- [apache](#)
- [Lighttpd Clean URLs](#)
- [Operating System independence](#)
- [php.ini](#)
- [Upload file size](#)
- [Apache Clean URLs](#)
- [php.ini](#)
- <http://www.htaccessredirect.net/>

Alias names for this page:

---

[\\_htaccess](#) | [.htaccess](#)