The PHP Advanced Editor

(*WHM >> Home >> Service Configuration >> PHP Configuration Editor*)

Overview

The *PHP Configuration Advanced Editor* includes all PHP configuration options that are available for your version of PHP.

Directives List

You should exercise extreme caution when changing any of the values as this could result in non-functioning PHP scripts.

Click *Save* after you make your changes.

This is not an exhaustive list; please consult the PHP documentation above for more information.

Directive	Description
extension_dir	Assigns a directory for PHP extensions. These extensions contain functions that a PHP script can call when your server executes it
include_path	Lists a path or paths where your PHP functions will look for files when a script calls certain functions. You can separate the directory paths with a colon (:) in a *nix system or a semicolon (;) in the Windows® environment. (For example: `.:/example/path1:/example/path2`)
file_uploads	Describes whether HTTP file uploads are possible for your PHP scripts. Select *Off* to disallow file uploads or *On* to allow them. This directive defaults to *On*.
asp_tags	Allows PHP scripts to use ASP-like tags in addition to the usual tags. This includes the variable-value printing shorthand of <%= $value %>.
memory_limit	Limits the amount of memory that scripts can allocate, described in bytes. This aids in preventing poorly written scripts from using too much memory. Use the character 'M' to define the limit in Megabytes. (For example: ***32M*** limits the allocation of memory to 32 Megabytes - the default setting.)
post_max_size	Specifies how much data your server allows PHP to take from a user via post requests through Apache.
register_globals	This defines whether or not your server allows the following variables to be defined as global: Environment, GET, POST, Cookie, and Server. Global variables are accessible at every level of the application. Select *Off* or *On*. This directive defaults to *Off*. **Warning:** This is a deprecated feature that, if you enable it, poses serious security risks for your server. We **strongly** recommend that you leave this directive set to *Off*.
upload_max_filesize	Defines the maximum file size for an upload in bytes. Use the character 'M' to define the limit in Megabytes. (For example: *2M* limits the file size to two Megabytes — the default setting.)
upload_tmp_dir	Specifies the directory for storing temporary files that users upload through PHP.

display_errors	Selects whether to display errors that occur during the execution of a PHP script. If you enable this feature, it may expose your server to some security risks. When your server displays the error information, an attacker can view valuable information about the error. In most cases this option should be left disabled. Use log_errors and error_log instead.
error_log	Defines the path to the error log file. You should use this log file to check errors rather than using *display_errors*.
error_reporting	Defines the level of error that your server records.
log_errors	Selects whether to log the errors that occur when your server executes a PHP script. This is preferable to, and more secure than, *display_errors*.
allow_url_fopen	Enables or disables the `fopen()` function. This function is responsible for accessing remote files. We do not recommend that you enable `fopen()` due to the security risk.
max_execution_time	Defines, in seconds, the maximum amount of time that your server allows a script to run before your server terminates it. This feature prevents excessive CPU usage on your server by poorly written scripts. This directive defaults to `30`.
disable_functions	Allows you to disable PHP functions that you do not want enabled on your server. To use this feature, enter the function name separated by a comma (**,**). (Example: `function1, function2...`) *Safe Mode* does not affect this feature.
max_input_time	Defines the maximum amount of time, in seconds, your server allows a script to parse input data. This directive defaults to *60*.
enable_dl	If you set this directive to *On*, it allows users to employ the `dl` function in their scripts, which dynamically loads a PHP extension at runtime. **Warning:** If you set this directive to *On* , it poses security risks to your server. We recommend you turn it *Off* unless it is absolutely necessary that you enable it.
safe_mode	This feature prevents the execution of a PHP script by a user that does not own the script. For example, if the user cPanel1 owns example.php, your server will not allow a user known by another alias to execute example.php.
open_basedir	**Warning:** *Do not edit this option*. Apache configures the `open_basedir` option.
safemode_includedir	Defines a directory that `safe_mode` does not affect. You should add your PEAR and PECL libraries to this directory. You should add your PEAR and PECL libraries to this directory.
session.save_path	Defines the path where your server stores files created by PHP. If you use the default handler, the default value is `/tmp`.

sql.safe_mode	**Warning:** Do *not* enable this feature unless absolutely necessary. This will prevent users who do not own the database from accessing the database. The net effect will be the failure of many programs and applications, such as shopping carts or content managers, that access databases for normal operation.

Additional documentation

Suggested documentationFor cPanel usersFor WHM usersFor developers

- Tweak Settings - PHP
- cPanel PHP
- Configuration Values of PHP-FPM
- PHP-FPM User Pools
- Scripts and Scripting Languages FAQ

- PHP
- PHP PEAR Packages
- MultiPHP INI Editor for cPanel
- MultiPHP Manager for cPanel

- How to Manage Your php.ini Directives with PHP-FPM
- Tweak Settings - PHP
- PHP Security Concepts
- How to Harden PHP
- Create Custom PHP Directives

- UAPI Functions - LangPHP::php_get_impacted_domains
- WHM API 1 Functions - php_fpm_config_set
- WHM API 1 Functions - php_fpm_config_get
- WHM API 1 Functions - php_set_system_default_version
- WHM API 1 Sections - PHP