



Looks like some of these free enhancements have been useful for your site?

Please consider supporting ASE.

"Very handy plugin by a great dev. Reported a bug yesterday, it was fixed today. Can't ask for better than that." ~[Greg Mount](#)

"So many useful features it blows my mind, as well as enabling me to ditch so many other plugins." ~[@simonclay](#)

FIND OUT HOW ▼

Content Management

Admin Interface

Log In | Log Out

Custom Code

Disable Components

Security

Optimizations

Utilities

Limit Login Attempts



Prevent brute force attacks by limiting the number of failed login attempts allowed per IP address.

failed login attempts allowed before 15 minutes
lockout

lockout(s) will block further login attempts for 24
hours

Failed login attempts:

Show entries

Search:

IP Address	Attempts	Last
Last Username	Lockouts	Attempt On
No data available in table		

Showing 0 to 0 of 0 entries

Previous

Next

COLLAPSE ▲

Obfuscate Author Slugs



Obfuscate publicly exposed author page URLs that shows the user slugs / usernames, e.g. *sitename.com/author/username1/* into *sitename.com/author/a6r5b8ytu9gp34bv/*, and output 404 errors for the original URLs. Also obfuscates in */wp-json/wp/v2/users/* REST API endpoint.

Email Address Obfuscator



Obfuscate email address to prevent spam bots from harvesting them, but make it readable like a regular email address for human visitors.

Use a shortcode like the following examples to display an email address on the frontend of your site:

- `[obfuscate email="john@example.com"]` to display the email on it's own line
- `[obfuscate email="john@example.com" display="inline"]` to show the email inline

COLLAPSE ▲

Disable XML-RPC



Protect your site from brute force, DOS and DDOS attacks via [XML-RPC](#). Also disables trackbacks and pingbacks.