Akeeba Admin Tools

20-06-2020

Online versie bij Akeeba: https://www.akeebabackup.com/documentation/admin-tools/waf-log.html#waf-log-reasons

List of blocking reasons

The block reasons, listed in the log and optionally sent to you by email are the following. The "Code" is what you need to enter in the "Do not log these reasons" or "Do not send email notifications for these reasons" options in WAF configuration to prevent these security exceptions from being logged or trigger an email respectively.

404 Shield

Code: `404shield`

See the Configure WAF page, **404 Shield**. The request was blocked by Admin Tools.

Admin Query String

Code: `adminpw`

Someone tried to access your site's administrator section but he didn't provide the secret URL parameter. Admin Tools blocked him and prevented him from seeing the login page at all.

Admin Exlusive Allow IP List

Code: `ipwl`

Someone tried to access your site's administrator section but his IP was not in the Administrator Exclusive Allow IP List. Admin Tools blocked him and prevented him from seeing the login page at all.

Site IP Disallow List

Code: not applicable

Someone tried accessing the front- or back-end of your site but his IP is in the IP Disallow List. Admin Tools blocked him and didn't allow him to see the content of your site.

SQLi Shield

Code: `sqlishield`

See the Configure WAF page, **SQLiShield protection against SQL injection attacks**. The attack was blocked by Admin Tools.

Bad Words Filtering

Code: `antispam`

The request contains one of the Bad Words you have defined and was blocked by Admin Tools.

tp=1 in URL

Code: not applicable

Only for Joomla! 1.5, see the respective option in the Configure WAF page. The attack was blocked by Admin Tools.

tmpl= in URL

Code: `tmpl`

See the Configure WAF page, **Block tmpl=foo system template switch**. The attack was blocked by Admin Tools.

template= in URL

Code: `template`

See the Configure WAF page, **Block template=foo site template switch**. The attack was blocked by Admin Tools.

MUA Shield

Code: `muashield`

See the Configure WAF page, **Malicious User Agent block (MUAShield)**. The attack was blocked by Admin Tools.

CSRF Shield

Code: `csrfshield`

See the Configure WAF page, **CSRF/Anti-spam form protection (CSRFShield)** . The attack was blocked by Admin Tools.

Bad Behaviour

Code: not applicable

See the Configure WAF page, **Bad Behaviour integration**. The attack was blocked by Admin Tools. NO LONGER PRESENT SINCE ADMIN TOOLS 2.5.3

RFIShield

Code: `rfishield`

See the Configure WAF page, **Remote File Inclusion block (RFIShield)**. The attack was blocked by Admin Tools.

DFIShield

Code: `dfishield`

See the Configure WAF page, **Direct File Inclusion shield (DFIShield)**. The attack was blocked by Admin Tools.

UploadShield

Code: `uploadshield`

See the Configure WAF page, **Uploads scanner (UploadShield)**. The attack was blocked by Admin Tools.

XSSShield

Code: `xssshield`

(Only on older sites) **Cross Site Scripting block (XSSShield)**. The attack was blocked by Admin Tools. This has been removed in Admin Tools 3.6.7 as it was throwing too many false positives (legitimate requests being blocked).

Spammer (via HTTP:BL)

Code: `httpbl`

See the Configure WAF page, **SQLiShield protection against SQL injection attacks**. The attack was blocked by Admin Tools.

Login failure

Code: `loginfailure`

Someone tried to log in in the front- or back-end of your site with the wrong username and/or password.

Two-factor Auth Fail

Code: `securitycode`

Someone tried to log in the back-end of your site but provided the wrong Two Factor Authentication code. Please note that this feature has been removed since Admin Tools 3.5.0. If you see it, it probaby comes from an old version of Admin Tools.

Backend Edit Admin User

Code: `nonewadmins`

Someone tried to create or edit an administrator user from the backend of your site. In this context "administrator user" means any user who belong in one or more User Groups that gives them backend login privileges. In a default Joomla! installation these are the users belonging to the Manager, Administrator and Super User groups.

Frontend Edit Admin User

Code: `nonewfrontendadmins`

Someone tried to create or edit an administrator user from the frontend of your site. In this context "administrator user" means any user who belong in one or more User Groups that gives them backend login privileges. In a default Joomla! installation these are the users belonging to the Manager, Administrator and Super User groups.

Configuration Editing

Code: `configmonitor`

Someone tried to change either the Global Configuration of Joomla! itself or the configuration (Options) of a component. Please consult the additional information saved with this security exception to understand which configuration was attempted to be changed. The change may have originated from the backend or the frontend of your site.