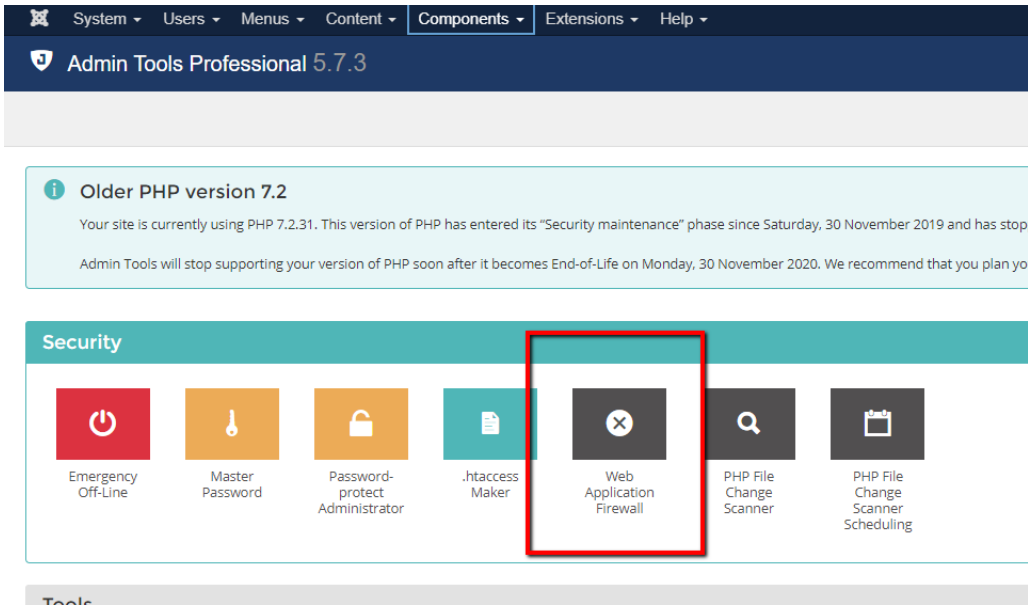


AdminTools - Blacklist an IP Address and set security notification emails

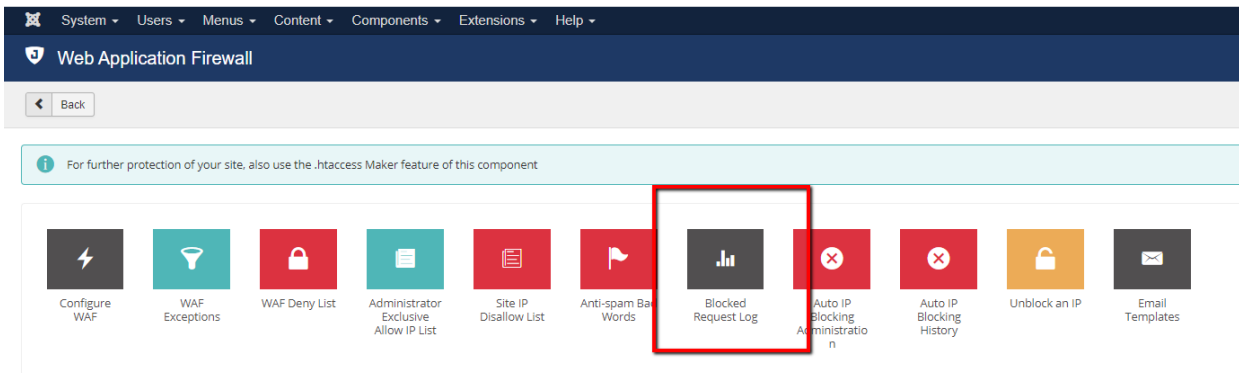
Please do not edit any other settings in your firewall aside from blacklisting IPs and setting the notification email(s).

To access the firewall, please navigate to **Components > AdminTools**

Select **Web Application Firewall**

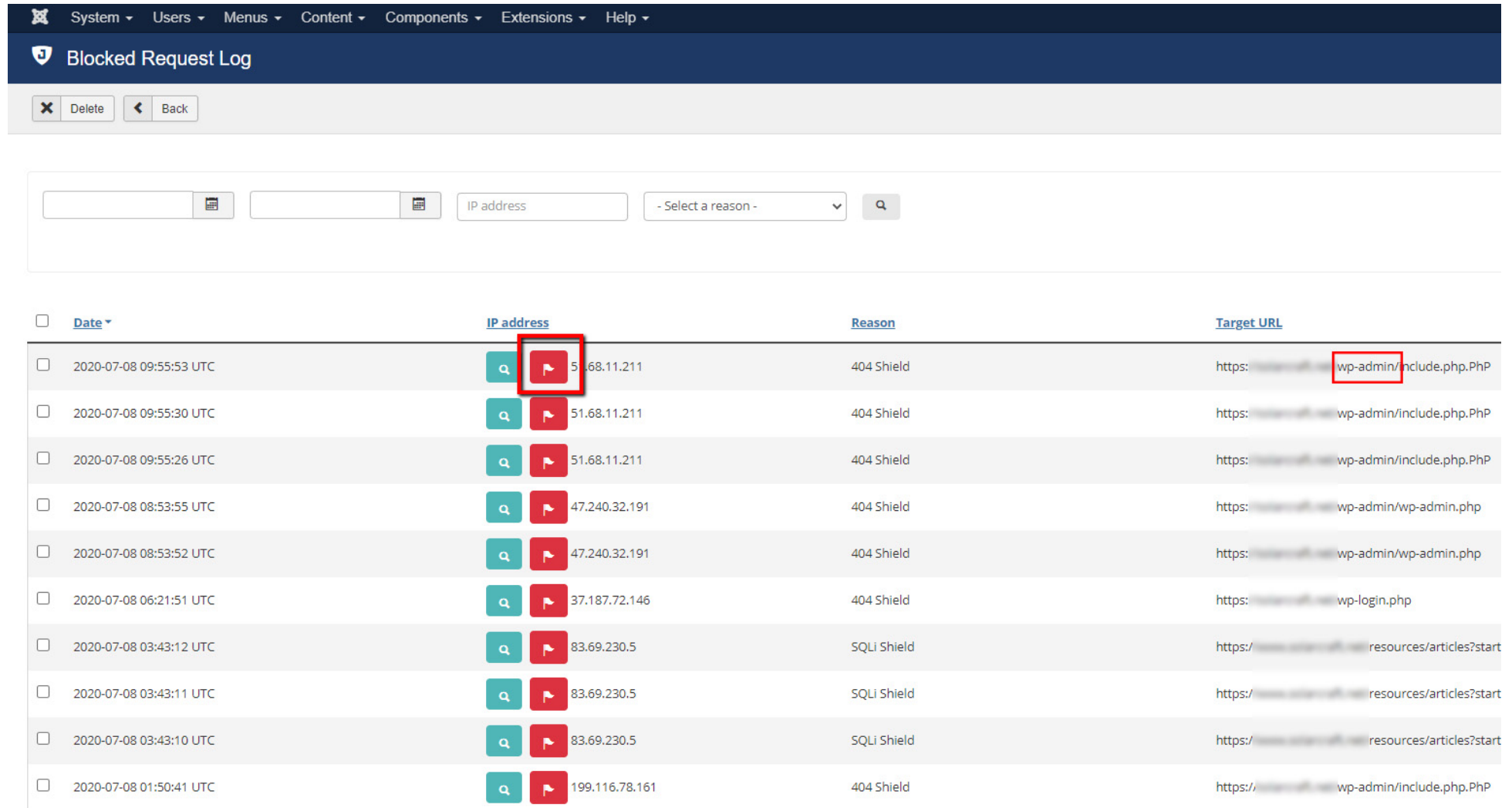


To view the list of suspicious IP addresses and the reason they triggered the firewall, select **Blocked Request Log**.



AdminTools - Blacklist an IP Address and set security notification emails

You can review the blocked requests and manually blacklist an IP Address.
To blacklist, **select the red flag button** beside the IP Address.



The screenshot displays the 'Blocked Request Log' interface. At the top, there is a navigation bar with 'System', 'Users', 'Menus', 'Content', 'Components', 'Extensions', and 'Help' menus. Below this is a header for 'Blocked Request Log' with 'Delete' and 'Back' buttons. A search bar is present with fields for 'IP address' and '- Select a reason -'. The main content is a table with the following columns: 'Date', 'IP address', 'Reason', and 'Target URL'. The table contains ten rows of blocked requests. The first row is highlighted, and a red flag icon is visible next to the IP address '51.68.11.211'. The 'Target URL' for this row is 'https://www.akeebabackup.com/wp-admin/include.php,PhP', where 'wp-admin/include.php,PhP' is also highlighted with a red box.

Date	IP address	Reason	Target URL
2020-07-08 09:55:53 UTC	51.68.11.211	404 Shield	https://www.akeebabackup.com/wp-admin/include.php,PhP
2020-07-08 09:55:30 UTC	51.68.11.211	404 Shield	https://www.akeebabackup.com/wp-admin/include.php,PhP
2020-07-08 09:55:26 UTC	51.68.11.211	404 Shield	https://www.akeebabackup.com/wp-admin/include.php,PhP
2020-07-08 08:53:55 UTC	47.240.32.191	404 Shield	https://www.akeebabackup.com/wp-admin/wp-admin.php
2020-07-08 08:53:52 UTC	47.240.32.191	404 Shield	https://www.akeebabackup.com/wp-admin/wp-admin.php
2020-07-08 06:21:51 UTC	37.187.72.146	404 Shield	https://www.akeebabackup.com/wp-login.php
2020-07-08 03:43:12 UTC	83.69.230.5	SQLi Shield	https://www.akeebabackup.com/resources/articles?start
2020-07-08 03:43:11 UTC	83.69.230.5	SQLi Shield	https://www.akeebabackup.com/resources/articles?start
2020-07-08 03:43:10 UTC	83.69.230.5	SQLi Shield	https://www.akeebabackup.com/resources/articles?start
2020-07-08 01:50:41 UTC	199.116.78.161	404 Shield	https://www.akeebabackup.com/wp-admin/include.php,PhP

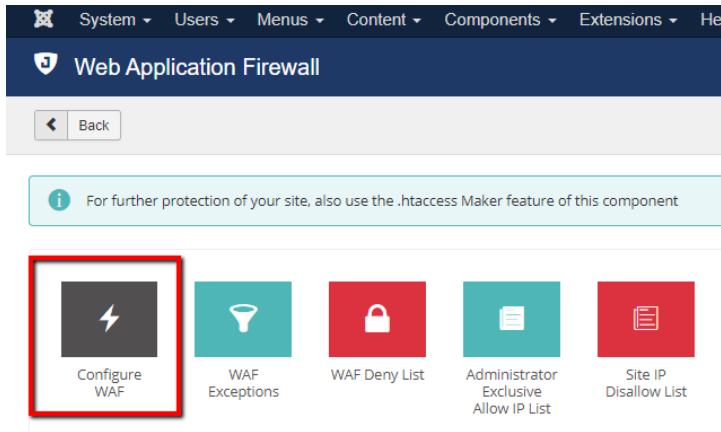
Some attempts are obviously malicious such as attempts to access "wp-admin" URLs (WordPress admin link) for the Joomla site.

This is the full list of reasons AdminTools will block a request:

<https://www.akeebabackup.com/documentation/admin-tools/waf-log.html#waf-log-reasons>

AdminTools - Blacklist an IP Address and set security notification emails

To set up security notification emails, navigate to **Components > AdminTools > Web Application Firewall**
Select **Configure WAF**



On the **Logging & Reporting** tab you can set notification emails.
Enter one or more email addresses (separated by commas) which will get notified in these fields.
Select **Save & Close** to save the adjusted settings.

