AMNESTY INTERNATIONAL

Joomla!®

Maintain. Protect. Optimise.
Admin Tools for Joomla!

AMNESTY – INTERNETGROEP

Joomla beveiliging

Donderdag 18 november 2021

Richard de Boer

Joomla beveiliging

Agenda

- Inleiding & aanleiding
- Waarom Admin Tools? - pluspunten
- Installatie / aanmelden na Admin Tools
- Admin Tools gebruiken
- Web Application Firewall
- Logging & Statistics
- Admin Tools E-mails

Joomla beveiliging

Inleiding & aanleiding

- In 2019 aantal hack-pogingen groepen sites
- Consequenties voor enkele groepensites
- Ook gevolgen voor Amnesty.nl
  - <groepensite>.amnesty.nl verdacht / besmet
  - www.amnesty.nl ook verdacht /besmet!
- WordPress – Wordfence
- Joomla – Akeeba Admin Tools

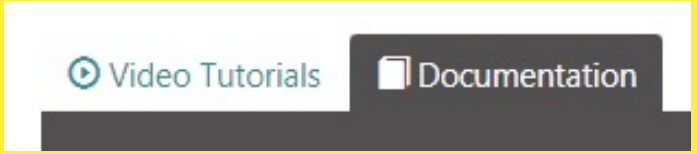
Joomla beveiliging

Akeeba Admin Tools

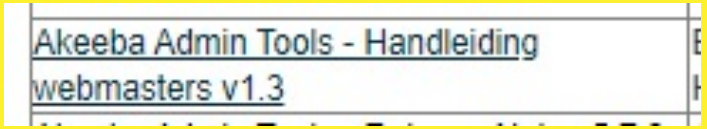
Maintain. Protect. Optimise.
Admin Tools for Joomla!

“Admin Tools is een software bundel die bestaat uit een Joomla! component, een module en een plug-in met als voornaamste doel de veiligheid en de prestaties van uw website te verbeteren, evenals de beheerder van deze website het leven een stuk makkelijker te maken door het automatiseren van algemene taken.”

https://www.akeebabackup.com/support/admin-tools/Tickets.html



https://internetgroep.amnesty.nl/images/downloadables/Akeeba_Admin_Tools_-_Handleiding_Amnesty_Webmasters.pdf



Joomla beveiliging

Akeeba Admin Tools - pluspunten

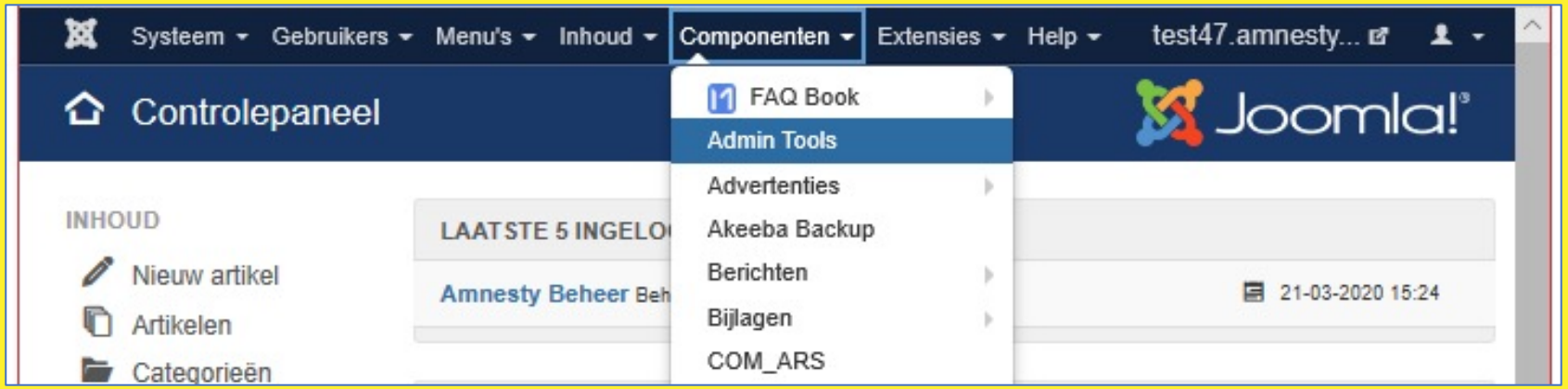
- De Web Application Firewall
- (Automatische) Blokkade van schadelijke IP adressen
- Toestaan veilige IP adressen (voor beheerders, Allow IP List)
- Automatisch controleren van de site (bestanden, rechten, wijzigingen)
- Gedetecteerde meldingen worden gelogd
- Meldingen kunnen worden verstuurd per mail
- Afscherming voor centraal beheer en lokale webmaster

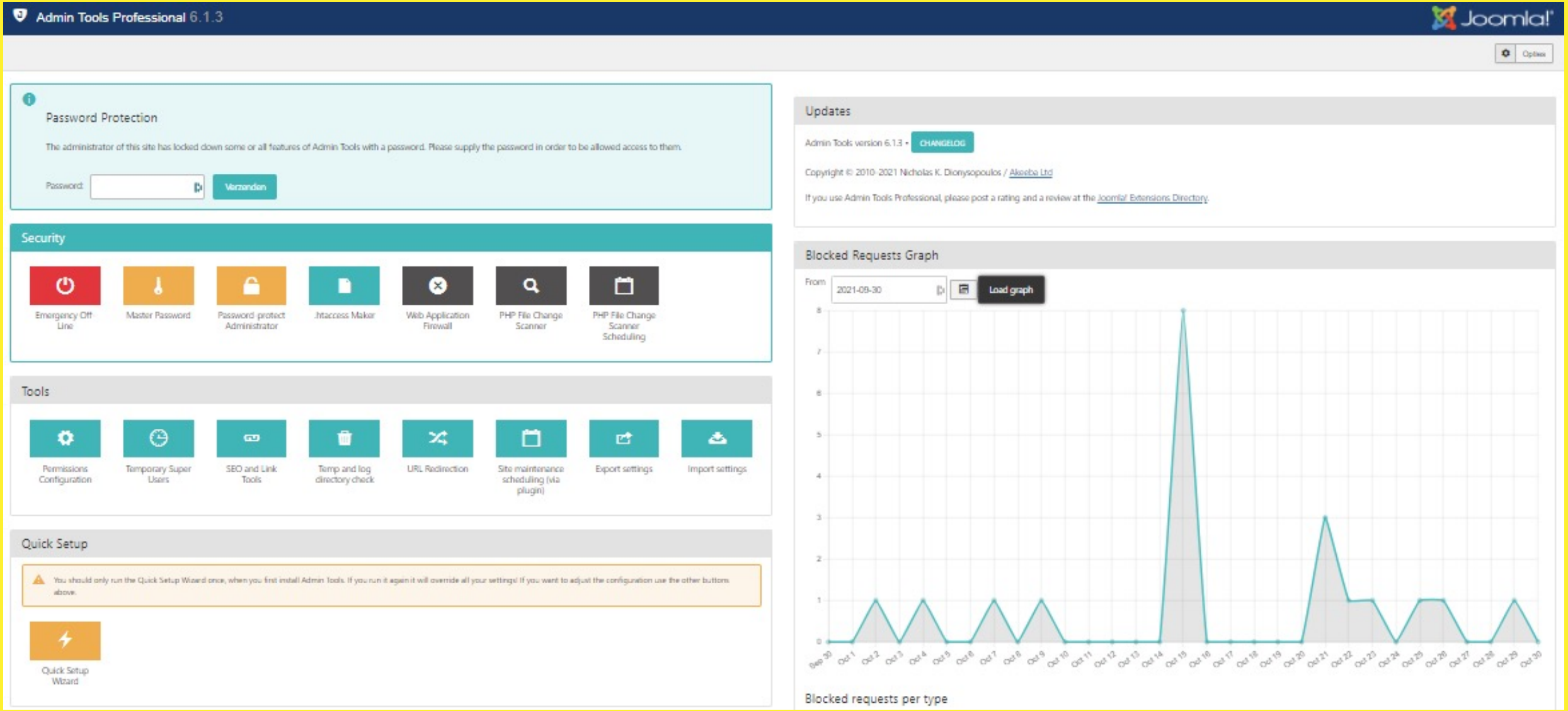
Joomla beveiliging

Installatie / aanmelden

Maintain. Protect. Optimise.
Admin Tools for Joomla!

- Installatie door de Internetgroep / webhosting
- Aangepaste Administrator Loging
  - https://<sitenaam>.amnesty.nl/administrator/index.php?<string>
  - Bij extra IP beveiliging ook zonder extra string
-




Admin Tools Professional 6.1.3
Joomla!
Options
Password Protection
The administrator of this site has locked down some or all features of Admin Tools with a password. Please supply the password in order to be allowed access to them.
Password:
Verzenden
Security
Emergency Off Line
Master Password
Password protect Administrator
.htaccess Maker
Web Application Firewall
PHP File Change Scanner
PHP File Change Scanner Scheduling
Tools
Permissions Configuration
Temporary Super Users
SEO and Link Tools
Temp and log directory check
URL Redirection
Site maintenance scheduling (via plugin)
Export settings
Import settings
Quick Setup
You should only run the Quick Setup Wizard once, when you first install Admin Tools. If you run it again it will override all your settings! If you want to adjust the configuration use the other buttons above.
Quick Setup Wizard
Updates
Admin Tools version 6.1.3
CHANGELOG
Copyright © 2010-2021 Nicholas K. Dionysopoulos / Akeeba Ltd
If you use Admin Tools Professional, please post a rating and a review at the Joomla! Extensions Directory.
Blocked Requests Graph
From
2021-09-30
Load graph
Blocked requests per type

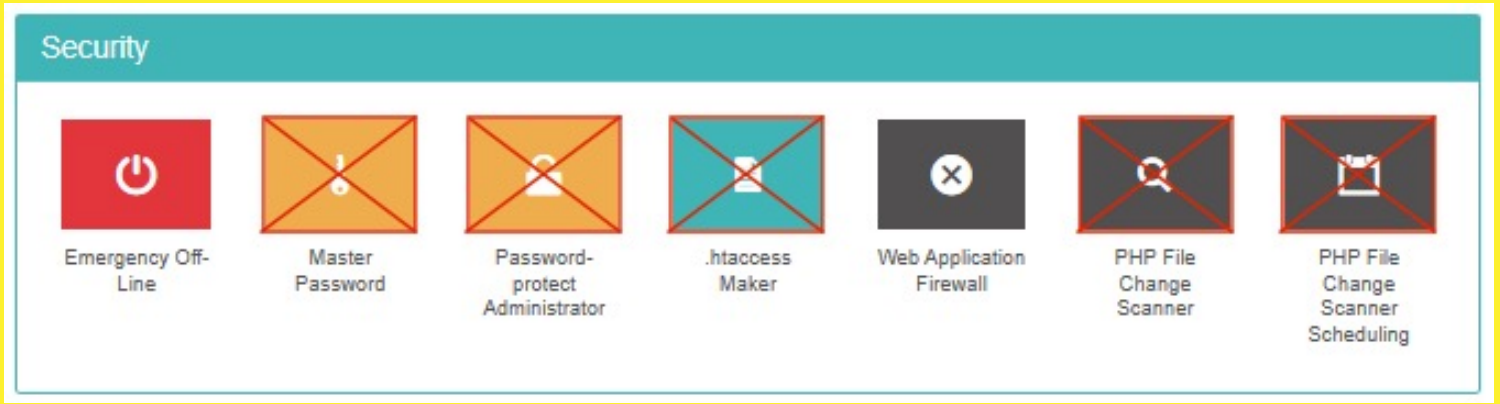
Joomla beveiliging

Control panel

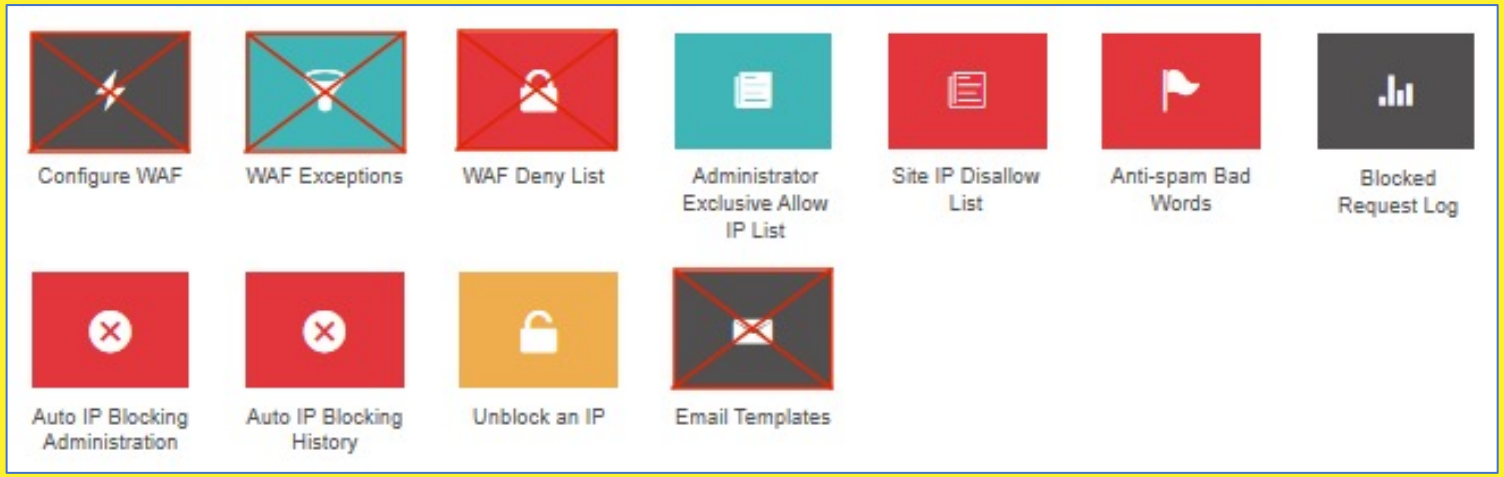
Maintain. Protect. Optimise.

Admin Tools for Joomla!

- Security



- Web Application Firewall

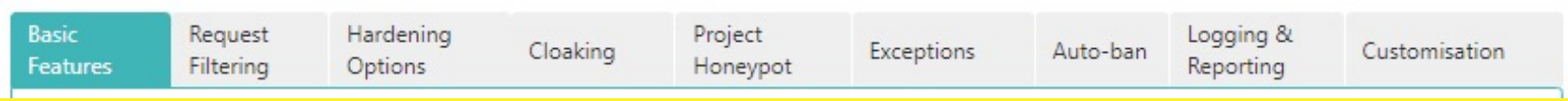


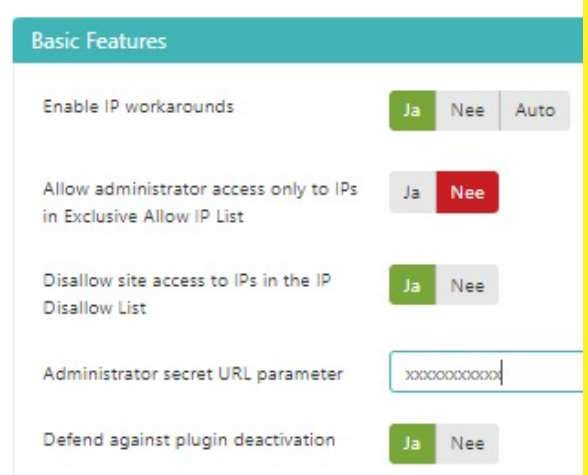
Joomla beveiliging

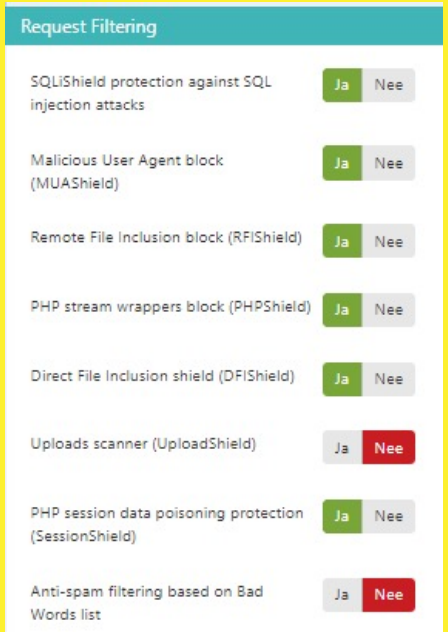
Configure Web Application Firewall

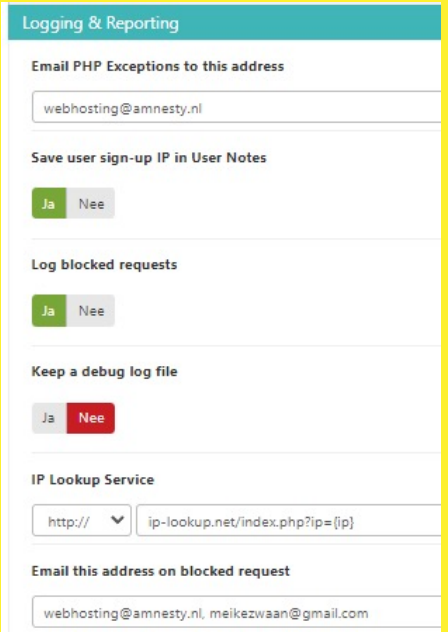
Maintain. Protect. Optimise.
Admin Tools for Joomla!

- Basis configuratie voor je gedaan





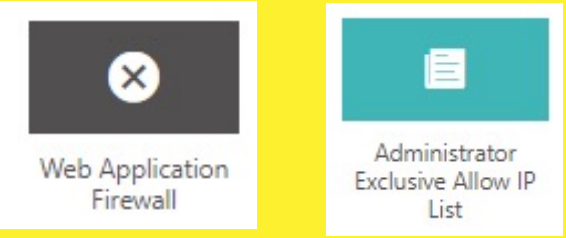


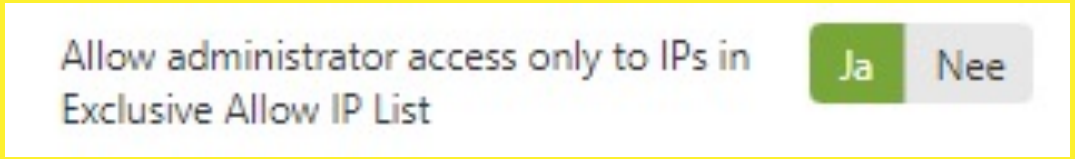


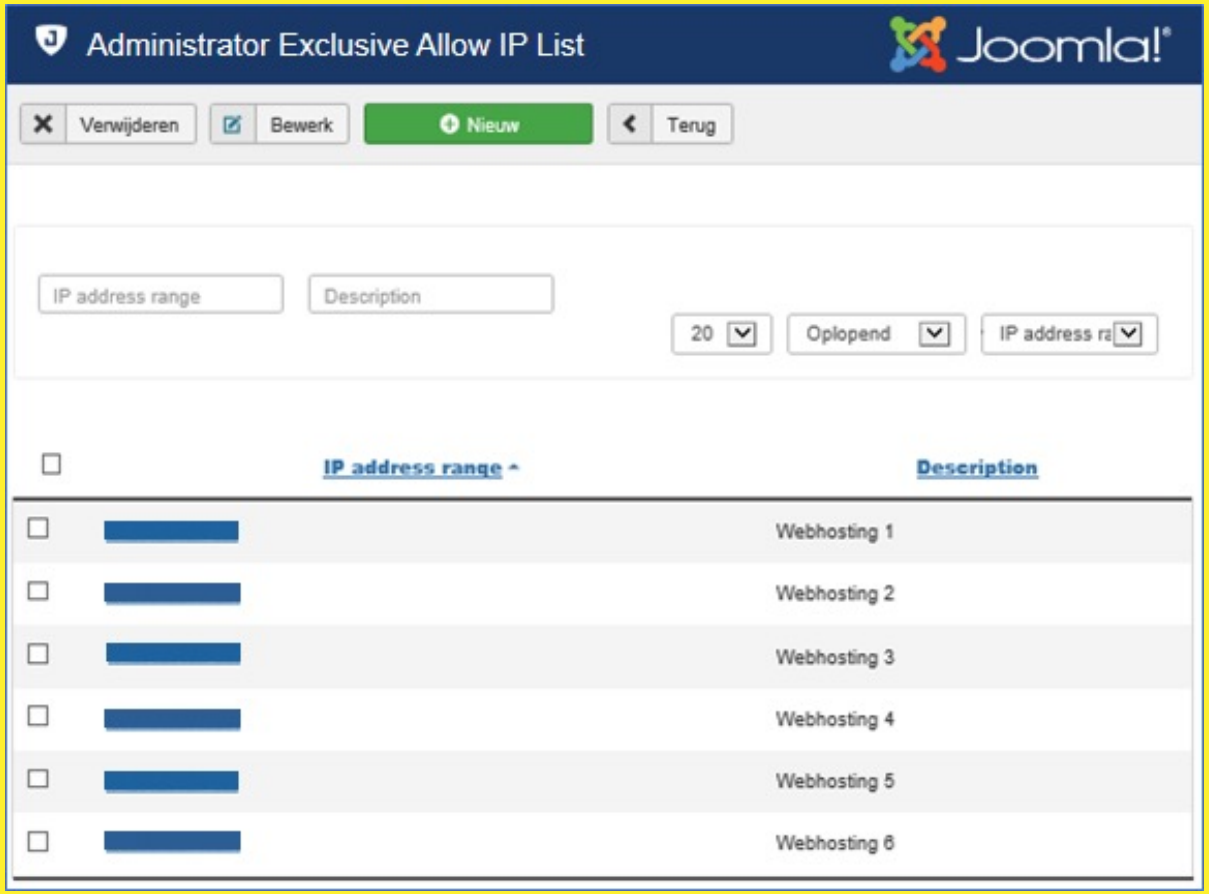
Joomla beveiliging

Extra IP beveiling adminstrators

Maintain. Protect. Optimise.
Admin Tools for Joomla!

- 

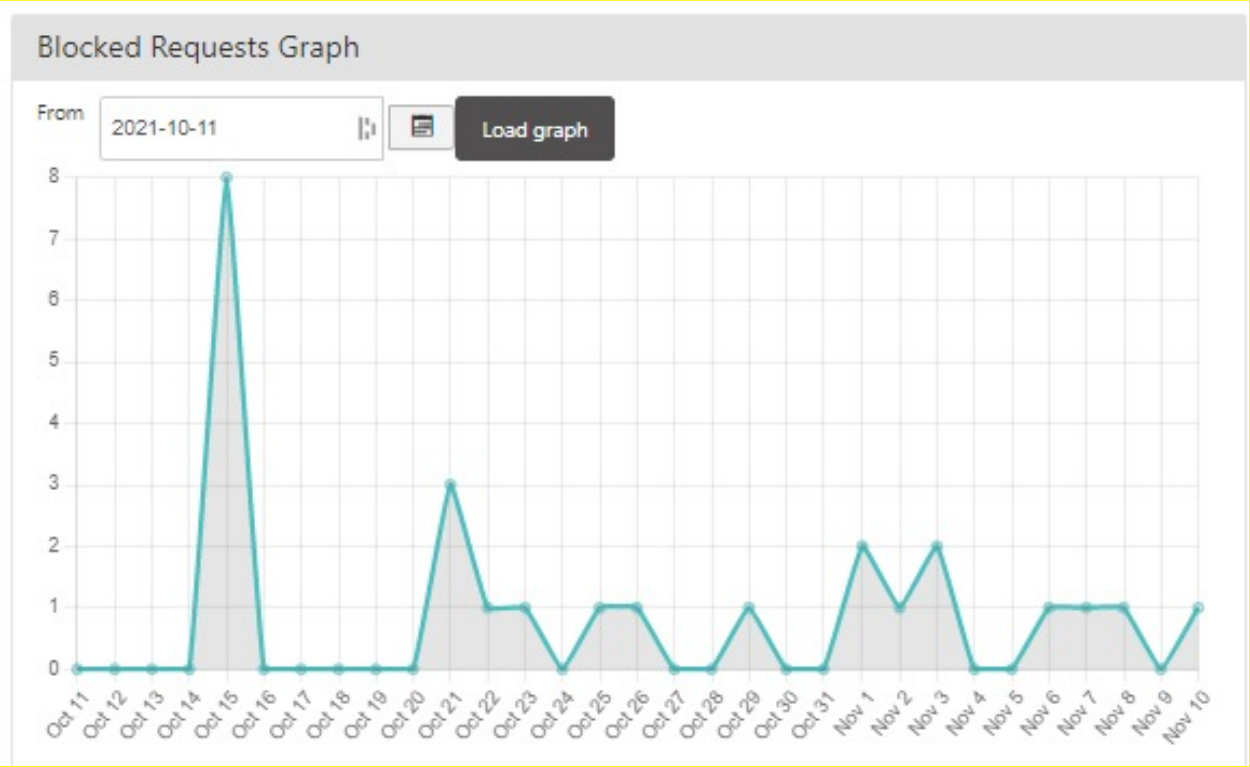


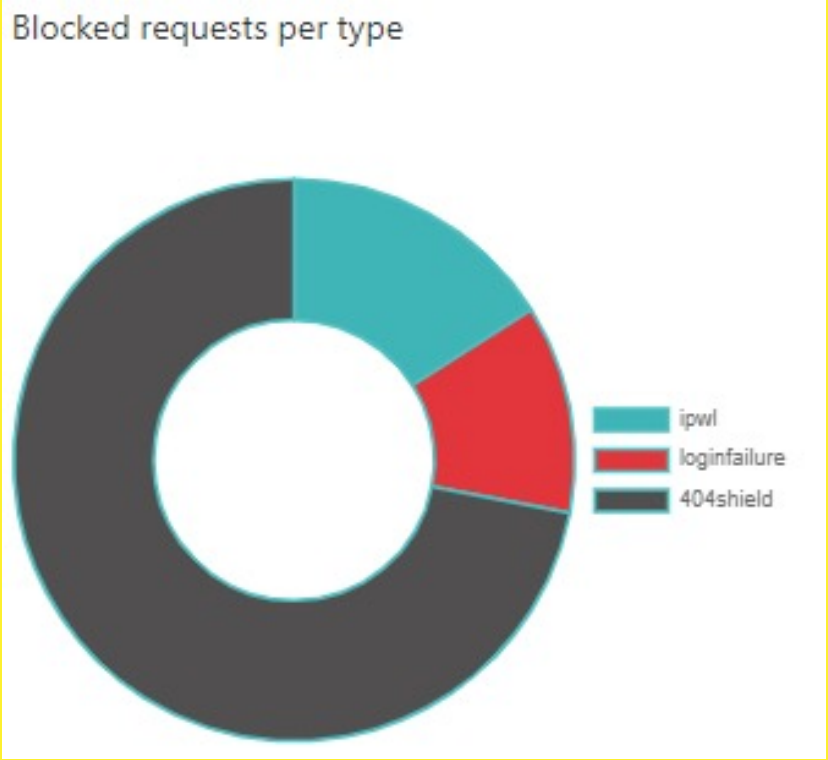


- Even aanvragen bij webhosting

Joomla beveiliging
Logging & Statistics 1

Maintain. Protect. Optimise.
Admin Tools for Joomla!





Joomla beveiliging
Logging & Statistics 2

Maintain. Protect. Optimise.
Admin Tools for Joomla!

Date	IP address	Reason	Target URL
2021-11-10 16:44:05 CET	37.0.11.64	404 Shield	https://internetgroep.amnesty.nl/wp-admin/css/
2021-11-08 05:02:15 CET	35.225.94.95	404 Shield	https://internetgroep.amnesty.nl/wp-login.php
2021-11-07 16:50:15 CET	94.212.194.253	Login failure	https://internetgroep.amnesty.nl/service2/webhostir
2021-11-06 04:32:30 CET	165.227.115.229	404 Shield	https://internetgroep.amnesty.nl/wp-login.php
2021-11-03 18:13:58 CET	156.146.49.139	404 Shield	https://internetgroep.amnesty.nl/wp-login.php
2021-11-03 02:00:57 CET	67.205.3.168	404 Shield	https://internetgroep.amnesty.nl/wp-login.php
2021-11-02 18:02:32 CET	159.89.1.19	404 Shield	https://internetgroep.amnesty.nl/wp-login.php
2021-11-01 12:16:13 CET	154.21.208.153	404 Shield	https://internetgroep.amnesty.nl/wp-login.php
2021-11-01 03:59:08 CET	164.68.110.108	404 Shield	https://internetgroep.amnesty.nl/wp-login.php

Joomla beveiliging
Admin Tools E-mail

Maintain. Protect. Optimise.
Admin Tools for Joomla!

Reason	Subject	Gepubliceerd	Language
all	Admin Tools melding voor [SITENAME]	✓	Alle
user-reactivate	Admin Tools melding Gebruiker geblokkeerd voor [SITENAME]	✓	Alle
adminloginfail	Admin Tools melding Mislukte administrator login [USER] voor [SITENAME]	✓	Alle
adminloginsuccess	Admin Tools melding voor [SITENAME] Administrator [USER] login	✗	Alle
ipautoban	Admin Tools melding IP [IP] geblokkerd voor [SITENAME]	✓	Alle
configmonitor	Admin Tools melding Configuratie wijziging [AREA] voor [SITENAME]	✓	Alle
criticalfiles	Admin Tools melding Bestandswijzigingen voor [SITENAME]	✓	Alle
superuserslist	Super Users were added to [SITENAME]	✓	Alle
rescueurl	Admin Tools melding Rescue URL verzoek voor [SITENAME] gebruiker [USER]	✗	Alle
criticalfiles_global	Admin Tools melding Bestandswijzigingen voor [SITENAME]	✓	Alle

Do not send email notifications for these reasons

SQLi Shield ⊗ tmpl= in URL ⊗

template= in URL ⊗ MUA Shield ⊗

SessionShield ⊗ DFIShield ⊗

404 Shield ⊗

Microsoft Word - Akeeba Admin Tools - List of blocking reasons.docx

Joomla beveiliging

Admin Tools E-mail

Maintain. Protect. Optimise.

Admin Tools for Joomla!

VAN	ONDERWERP	VERZONDEN
Alphen a/d Rijn	Admin Tools melding IP 217.160.192.178 geblokkerd voor Alphen aan den Rijn	zo 7-11-2021 22:22
intrnetgroep.amnesty.nl	Admin Tools melding voor Internetgroep Amnesty NL	zo 7-11-2021 16:50
Culemborg Amnesty	Admin Tools melding Configuratie wijziging Algemene instellingen voor Culemborg...	zo 7-11-2021 12:27
Culemborg Amnesty	Admin Tools melding Bestandswijzigingen voor Culemborg-Amnesty	zo 7-11-2021 12:27
alkmaar	Admin Tools melding voor alkmaar	zo 7-11-2021 11:40
alkmaar	Admin Tools melding voor alkmaar	zo 7-11-2021 11:27
alkmaar	Admin Tools melding voor alkmaar	zo 7-11-2021 11:26
Amnesty Heerhugowaard	Admin Tools melding IP 54.147.178.243 geblokkerd voor Heerhugowaard	za 6-11-2021 21:57
leiden.amnesty.nl	Admin Tools melding IP 138.201.203.132 geblokkerd voor Leiden	za 6-11-2021 20:55
leiden.amnesty.nl	Admin Tools melding IP 138.201.203.132 geblokkerd voor Leiden	za 6-11-2021 20:36
leiden.amnesty.nl	Admin Tools melding IP 138.201.203.132 geblokkerd voor Leiden	za 6-11-2021 20:05
leiden.amnesty.nl	Admin Tools melding IP 138.201.203.132 geblokkerd voor Leiden	za 6-11-2021 19:49
test46	Joomla! Update available for test46 – https://test46.amnesty.nl/administrator/	za 6-11-2021 12:59
Amnesty Heerhugowaard	Admin Tools melding IP 54.147.178.243 geblokkerd voor Heerhugowaard	vr 5-11-2021 21:04
Amnesty Wierden	Admin Tools melding voor Amnesty Wierden	vr 5-11-2021 17:43
test46	Joomla! Update available for test46 – https://test46.amnesty.nl/administrator/	vr 5-11-2021 15:55
beheer,amnesty.nl	Admin Tools troubleshooting information	vr 5-11-2021 15:55
beheer,amnesty.nl	User Beheer@Amnesty20 (Amnesty Beheer <webhosting	vr 5-11-2021 15:54
test38.amnesty.nl	User Beheer@Amnesty20 (Amnesty Beheer <webhosting	vr 5-11-2021 15:50
beheer,amnesty.nl	Critical file modified on test42	vr 5-11-2021 14:47
beheer,amnesty.nl	Joomla! update beschikbaar voor test42-https://test42.amnesty.nl/administrator/	vr 5-11-2021 14:45
beheer,amnesty.nl	User Beheer@Amnesty20 (Amnesty Beheer <webhosting	vr 5-11-2021 14:45
test35.amnesty.nl	Admin Tools melding Bestandswijzigingen voor test35	vr 5-11-2021 14:41
Amnesty Wierden	Admin Tools melding IP 80.127.235.158 geblokkerd voor Amnesty Wierden	vr 5-11-2021 12:16

Email this address after an automatic IP ban

Email this address on blocked request

Email this address on failed administrator login

webhosting@amnesty.nl, meikezwaan@gmail.com

Aan NLD - INB - Webhosting

Hallo webmaster,

Er is een Admin Tools beveiligingsmelding voor de website **alkmaar** met de volgende details:
IP adres: **82.169.215.68** (IP Lookup: IP Lookup)
Reden: **Admin Query String**

Zie voor de reden ook de List of blocking reasons.

Met vriendelijke groet,
Webhosting Amnesty NL
webhosting@amnesty.nl

Je krijgt deze mail omdat je de administrator bent van alkmaar en omdat webhosting het ontvangen van deze mails zo voor je ingesteld heeft.

Joomla beveiliging

Vragen?