

Γνωσιακή βάση > cPanel / WHM > Πώς μπορώ να ενεργοποιήσω το Spam Assassin σε cPanel;

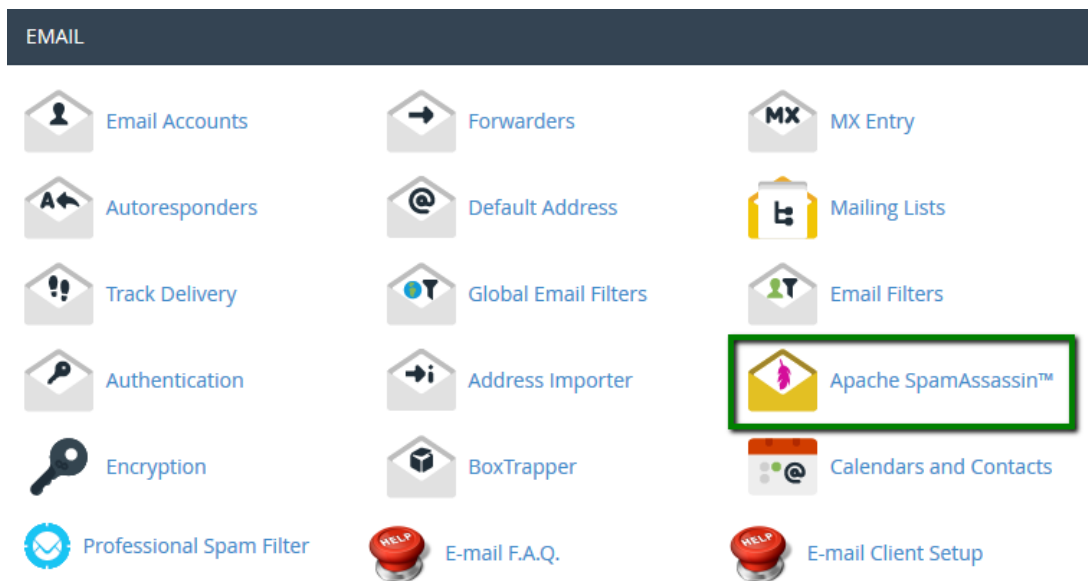
Πώς μπορώ να ενεργοποιήσω το Spam Assassin σε cPanel;

- 2019-03-07 - cPanel / WHM

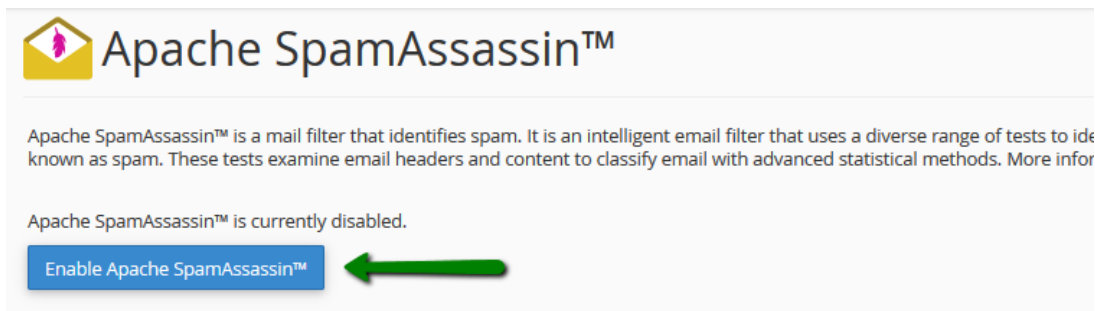
Το Apache SpamAssassin είναι ένα φιλικό προς τον χρήστη βοηθητικό πρόγραμμα ηλεκτρονικού ταχυδρομείου, το οποίο εξετάζει την εισερχόμενη αλληλογραφία για διαφορετικά χαρακτηριστικά ανεπιθύμητης αλληλογραφίας. Φιλτράρει τα ανεπιθύμητα μηνύματα και τα διαχωρίζει σε Spam ή όχι.

Για να ενεργοποιήσετε το SpamAssassin στον λογαριασμό σας, ακολουθήστε τα παρακάτω βήματα.

1. Συνδεθείτε στο cPanel σας και στην κατηγορία EMAIL κάντε click στο εικονίδιο Apache SpamAssassin.



2. Κάντε click στο Enable Apache SpamAssassin™ εικονίδιο.



Αφού το ενεργοποιήσετε, δείτε παρακάτω πώς μπορείτε να το διαχειριστείτε.

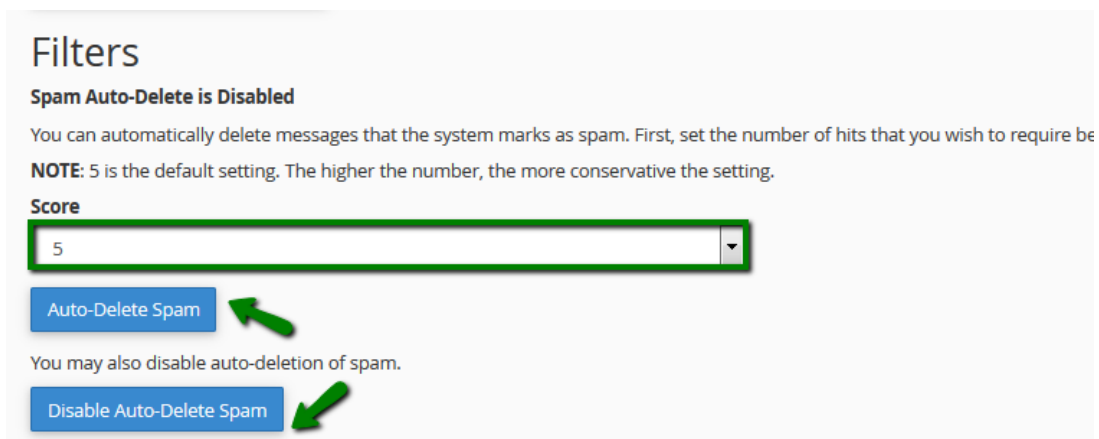
Φίλτρα

Η επιλογή αυτόματης διαγραφής ανεπιθύμητης αλληλογραφίας καταργεί αυτόματα τα μηνύματα ηλεκτρονικού ταχυδρομείου που πληρούν ή υπερβαίνουν το σύνολο αποτελεσμάτων spam. Για να το ορίσετε, μεταβείτε στο μενού Apache SpamAssassin και βρείτε το widget Φίλτρα.

Μπορείτε να ορίσετε το απαιτούμενο σκορ σε ένα αναπτυσσόμενο μενού (από το 1 έως το 10).

Για να ενεργοποιήσετε το φίλτρο, απλά κάντε click στο κουμπί Αυτόματη διαγραφή του Spam (Auto-Delete Spam).

Για να απενεργοποιήσετε το φίλτρο, κάντε click στην επιλογή Απενεργοποίηση αυτόματου διαγραφής spam (Disable Auto-Delete Spam)



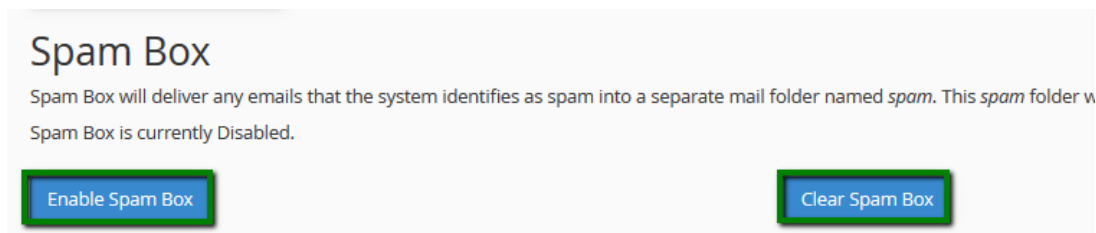
Spam Box

Το κουμπί Ενεργοποίηση κουτιού ανεπιθύμητης αλληλογραφίας (Enable Spam Box) κάνει το Exim να δημιουργήσει έναν φάκελο ανεπιθύμητης αλληλογραφίας (έναν ξεχωριστό φάκελο στο γραμματοκιβώτιό σας), ο οποίος θα συλλέγει εισερχόμενα μηνύματα που χαρακτηρίζονται ως spam.

ΣΗΜΕΙΩΣΗ: Ο φάκελος ανεπιθύμητης αλληλογραφίας ενδέχεται να μην εμφανίζεται από προεπιλογή. Αφού έχει ενεργοποιηθεί το Spam Box, θα χρειαστεί να ενεργοποιήσετε την

εμφάνισή του στις ρυθμίσεις του Webmail.

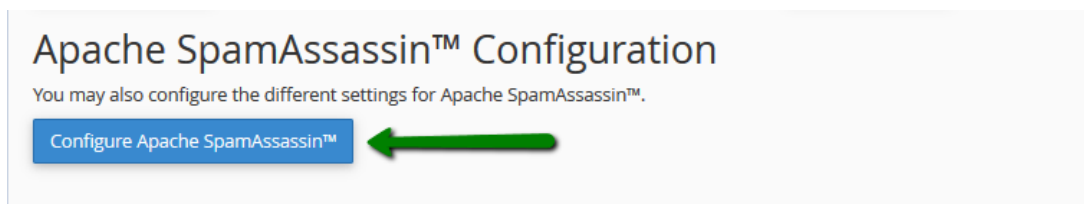
Είναι δυνατή η διαγραφή των μηνυμάτων που συλλέγονται από το Spam Box με ένα click στο κουμπί Εκκαθάριση κουτιού Spam (Clear Spam Box):



Ρύθμιση του Apache SpamAssassin

Κάθε εισερχόμενη αλληλογραφία προβάλλεται από το SpamAssassin και δίνεται μια βαθμολογία με βάση τα χαρακτηριστικά spam. Από προεπιλογή, μηνύματα ηλεκτρονικού ταχυδρομείου με σκορ 5 θεωρούνται ανεπιθύμητα. Ωστόσο, είναι δυνατό να προσαρμόσετε το φίλτρο ανάλογα με τις ανάγκες σας.

Για να το κάνετε αυτό, περιηγηθείτε στο widget Apache SpamAssassin™ Configuration και κάντε click στο Configure Apache SpamAssassin™ :



Θα μεταφερθείτε σε ένα μενού όπου διατίθενται πολλές επιλογές, για να ορίσετε τη δική σας βαθμολογία ανεπιθύμητης αλληλογραφίας. Βρείτε το πεδίο `required_score` και εισαγάγετε τη νέα τιμή:

Το `[new_score]` θα πρέπει να αντικατασταθεί με έναν αριθμό. Όλα τα εισερχόμενα μηνύματα που βαθμολογούνται με αυτόν τον αριθμό και υψηλότερα, θα σημειωθούν ως ανεπιθύμητα.

0 - σημαίνει ότι η οποιαδήποτε εισερχόμενη αλληλογραφία θα χαρακτηρίζεται ως ανεπιθύμητη αλληλογραφία.

5 - προκαθορισμένη βαθμολογία, λειτουργεί καλά για τους τυπικούς χρήστες.

ΣΗΜΕΙΩΣΗ: όσο χαμηλότερη είναι η βαθμολογία σας, τόσο πιο περιοριστικό θα είναι το φίλτρο.

Όταν τελειώσετε, κάντε click στην επιλογή Αποθήκευση (Save) στο κάτω μέρος της


σελίδας.

| | |
|---|--------------------------------|
| required_score | <input type="text" value="5"/> |
| <small>Assign scores (the number of points for a hit) to a given test. Scores can be positive or negative real numbers or integers. "SYM-BOLIC_TEST_NAME" is the symbolic name used by Apache SpamAssassin™ for that test; for example, 'FROM_ENDS_IN_NU'. If only one valid score is listed, then that score is always used for a test. If four valid scores are listed, then the score that is used depends on how Apache SpamAssassin™ is being used. The first score is used when both Bayes and network tests are disabled. The second score is used when Bayes is disabled, but network tests are enabled. The third score is used when Bayes is enabled and network tests are disabled. The fourth score is used when Bayes is enabled and network tests are enabled. Setting a rule's score to 0 will disable that rule from running.</small> | |
| score | <input type="text"/> |
| score | <input type="text"/> |
| score | <input type="text"/> |
| score | <input type="text"/> |
| score | <input type="text"/> |

Black List / White List

Ορισμένα μηνύματα ενδέχεται να εντοπιστούν λανθασμένα ως μη-spam από το Apache SpamAssassin. Αν αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου προέρχονται συχνά από τους συγκεκριμένους αποστολείς ηλεκτρονικού ταχυδρομείου, μπορείτε να τα απαριθμήσετε ως black. Το SpamAssassin θα επισημάνει τότε αυτά ως spam.

Για τη μαύρη λίστα συγκεκριμένων αποστολέων, απλώς εισάγετε το email αποστολής σε ένα από τα πεδία blacklist_from:

 **Apache SpamAssassin™**

Used to specify addresses which send mail that is often tagged (incorrectly) as non-spam, but which the user doesn't want. Same format as whitelist_from.

| | |
|-----------------------|----------------------|
| blacklist_from | <input type="text"/> |
| blacklist_from | <input type="text"/> |
| blacklist_from | <input type="text"/> |
| blacklist_from | <input type="text"/> |
| blacklist_from | <input type="text"/> |

Εάν το SpamAssassin συχνά αποκλείει ορισμένους αποστολείς ηλεκτρονικού ταχυδρομείου και επισημαίνει τα μηνύματά του ως ανεπιθύμητα (spam), είναι δυνατό να προσθέσετε τον αποστολέα στην White list.

Για να προσθέσετε στην White List έναν συγκεκριμένο αποστολέα, απλά εισάγετε το email

αποστολής σε ένα από τα πεδία `whitelist_from`:

Used to specify addresses which send mail that is often tagged (incorrectly) as spam; it also helps if they are addresses of big companies with lots of lawyers. This way, if spammers impersonate them, they'll get into big trouble, so it doesn't provide a shortcut around Apache SpamAssassin™. Whitelist and blacklist addresses are now file-glob-style patterns, so `friend@somewhere.com`, `*@isp.com`, or `*.domain.net` will all work. Specifically, `*` and `?` are allowed, but all other metacharacters are not. Regular expressions are not used for security reasons.

| | |
|-----------------------------|----------------------|
| <code>whitelist_from</code> | <input type="text"/> |
| <code>whitelist_from</code> | <input type="text"/> |
| <code>whitelist_from</code> | <input type="text"/> |
| <code>whitelist_from</code> | <input type="text"/> |
| <code>whitelist_from</code> | <input type="text"/> |

Save