Apache SpamAssassin

For cPanel & WHM version 64

(Home >> Email >> Apache SpamAssassin)

Overview

This interface allows you to configure Apache SpamAssassin™ for your account. Apache SpamAssassin is an email utility that examines incoming email and tests for spam characteristics. It uses Bayesian spam filtering and network tests to screen incoming email. This results in an overall score that Apache SpamAssassin uses to determine whether it should discard a message.

For more information, visit the Apache SpamAssassin website.

> **Note:**
> If you experience trouble when you use BoxTrapper and Apache SpamAssassin together, contact your web hosting provider for more information about your server's configuration.

Enable or disable Apache SpamAssassin

The *Apache SpamAssassin* interface displays the current status of the feature.

- To enable Apache SpamAssassin, click *Enable Apache SpamAssassin*™.
- To disable Apache SpamAssassin, click *Disable Apache SpamAssassin*™.

> **Note:**
> You **cannot** disable Apache SpamAssassin if your hosting provider enabled the *Apache SpamAssassin™: Forced Global ON* setting in WHM's *Apache SpamAssassin* interface (*Home >> Service Configuration >> Exim Configuration Manager*).

Filters

Spam Auto-Delete

The *Spam Auto-Delete* feature automatically deletes messages that meet or exceed the spam score limit.

- To enable this feature, select the desired minimum spam score and click *Auto-Delete Spam*. This setting defaults to *5*.
- To disable this feature, click *Disable Auto-Delete Spam.*

> **Note:**
> If you enable this feature and a message that is not spam meets or exceeds the defined score, you may lose that email. Make certain to properly configure Apache SpamAssassin before you use this feature.

Enable Spam Box

> **Warning:**
> If you check your mail through a POP3 client, access and empty your spam box with the username `youraddress@example.com/spam` and your email account password. If you do not delete email in the spam box frequently, spam may accumulate and cause you to reach your email account quota.
>
> - You **cannot** use this method to access other folders on your account. Some webmail clients may require additional steps. For more information, read our Apache SpamAssassin documentation.
> - If you are unsure whether you use POP3 or IMAP to receive mail, you can find this information in your email application's *P*

references interface.

Notes:

- Before you can use the spam box, your hosting provider **must** enable the *Enable Apache SpamAssassin™ Spam Box delivery for messages marked as spam* setting in WHM's *Tweak Settings* interface (*Home >> Server Configuration >> Tweak Settings*). To redirect spam from your email inbox, if this option is not available, create a spam email filter.
- We recommend that you enable this feature.
- If you **do not** enable the Spam Box feature but **do** enable Apache SpamAssassin, Apache SpamAssassin will deliver the message to the email account's inbox normally. You can create filters for these messages for all of your email accounts in cPanel's *Global Email Filters* interface (*Home >> Email >> Global Email Filters*), or for individual accounts in cPanel's *Email Filters* interface (*Home >> Email >> Email Filters*).

Click *Enable Spam Box* to cause Exim to create a `spam` folder the next time that you receive spam mail.

- Exim sends all of the mail that Apache SpamAssassin marks as spam to this folder.
- This feature preserves mail that the system may mistakenly classify as spam mail.

After you enable this feature, click *Clear Spam Box* to delete the messages in the spam box.

Apache SpamAssassin™ Configuration

Click *Configure Apache SpamAssassin™* to update Apache SpamAssassin's configuration.

Notes:

- Click *Save* to store your changes.
- To add more than five addresses to the blacklist or whitelist, enter addresses in the first five text boxes and click *Save*. Additional text boxes will appear.
- When you add addresses to the blacklist or whitelist, use `*` as a wildcard to represent multiple characters and `?` to represent a single-character wildcard. The following examples demonstrate how to properly use wildcards in the blacklist:
  - `user@example.com` — Blacklists or whitelists a single email address.
  - `*@example.com` — Blacklists or whitelists all of the addresses at `example.com`.
  - `?ser@example.com` — Blacklists or whitelists a single character in an address at `example.com` (for example, u`ser@example.com`, but not A`user@example.com`).

blacklist_from

Apache SpamAssassin may incorrectly tag some mail as non-spam messages. If these messages often come from specific addresses, you can blacklist them to ensure that Apache SpamAssassin tags their messages correctly.

To do this, enter the address in one of the *blacklist_from* text boxes.

Note:
To blacklist email addresses on multiple accounts, use the Exim System Filter File.

required_score

Apache SpamAssassin examines every email message for spam characteristics and assigns it an overall score.

Use the *required_score* text box to set the required score to mark a message as spam. The default setting is `5.0`, which is aggressive. This setting is suitable for a single user, but ISPs should set the default to be more lenient (for example, `8.0` or `10.0`).

score

Apache SpamAssassin uses hundreds of tests, and you can assign scores to individual tests to configure Apache SpamAssassin for your server.

To do this, perform the following steps:

1. To review the default scores, run the following command on the command line:

```
grep -R score /var/lib/spamassassin/* |less
```

2. You must know which version of Apache SpamAssassin runs on your server. To check your version of Apache SpamAssassin, run the following command:

```
/usr/local/cpanel/3rdparty/bin/spamassassin --version
```

3. Enter individual test scores in the *score* text boxes in the following format:

```
"score" "TEST_NAME" "1 or 4 positive or negative numbers"
```

The following table indicates when Apache SpamAssassin uses each score.

Score used	Bayes test	Network test
First Score	Disabled	Disabled
Second Score	Disabled	Enabled
Third Score	Enabled	Disabled
Fourth Score	Enabled	Enabled

Example

For example, you could enter the following individual test score:

```
score INVALID_DATE 3.2 3.3 2.5 2.1
```

This example sets the scores that Apache SpamAssassin assigns to a message with an invalid date in its header.

Notes:

- If you only list one number, the test uses that score.
- Set a score to `0` to disable the test.

In the example above, `3.2` is the first score, `3.3` is the second, `2.5` is the third, and `2.1` is the fourth. If you enter four numbers, as in the example, the score that Apache SpamAssassin uses depends on the enabled Bayes and network tests in your installation of Apache SpamAssassin.

whitelist_from

Add email addresses that Apache SpamAssassin often blocks, but from which you wish to receive mail, to the Apache SpamAssassin whitelist.

To do this, enter the address in one of the *whitelist_from* text boxes.