

# Spam Filters

(cPanel >> Home >> Email >> Spam Filters)

## Overview

This interface allows you to configure the spam filter settings (powered by Apache SpamAssassin™) for your account. Spam filters identify and sort or delete unsolicited email, commonly known as spam. You can also use this interface to configure your [whitelist](#) and [blacklist](#) settings.

For more information, read Apache SpamAssassin's [overview](#) documentation.

**Note:**

If you experience issues when you use [BoxTrapper](#) and Apache SpamAssassin simultaneously, contact your hosting provider for more information about your server's configuration.

## Process New Emails and Mark them as Spam

Set this toggle to enabled to identify potential spam. Apache SpamAssassin examines every message for spam characteristics and assigns them a calculated spam score. This calculated spam score helps determine the likelihood that a message contains spam. The [Spam Box](#) and [Auto-Delete](#) features require that you enable Apache SpamAssassin first.

**Note:**

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

## Spam Threshold Score

If the system calculates a spam score for a message that meets or exceeds the *Spam Threshold Score* setting, the system marks the message as spam. A lower spam threshold score, such as a one, is aggressive and labels many messages as spam, including messages that may **not** be spam. However, a higher value, such as a ten, is passive and only labels messages that are obviously spam.

To set the Spam Threshold value, perform the following steps:

1. Click the *Spam Threshold Score* link in the interface. The system directs you to the *Adjust Spam Threshold Score* interface.
2. Select the desired *Spam Threshold Score* from the menu.

**Note:**

Select *Custom* from the menu to enter a custom value.

3. Click *Update Scoring Options* to save your changes.

## Move New Spam to a Separate Folder (Spam Box)

Set this toggle to enabled to configure the Exim service to create a `spam` folder the next time that you receive spam mail. Spam Box sends any message with a calculated spam score that **exceeds** the Spam Threshold Score to this folder. This feature preserves email that Apache SpamAssassin may mistakenly classify as spam mail.

**Note:**

We recommend that you use Spam Box instead of Auto-Delete because you can still view the messages. However, you should occasionally empty this folder because the space that it uses counts towards your email quota limit.

### In This Document

### Related Documentation

- [Track Delivery](#)
- [Address Importer](#)
- [Global Email Filters](#)
- [Forwarders](#)
- [Email Filters](#)

### For Hosting Providers

- [How to Configure the Apache SpamAssassin Report\\_Safe Option](#)
- [The cPanel Update Configuration File - cpupdate.conf](#)
- [Common Mail Service IP Addresses](#)
- [Edit MX Entry](#)
- [Edit System Mail Preferences](#)

## Empty the Spam Box folder

To empty the spam folder or remove selected messages, click *Configure Spam Box Settings*. The system directs you to the *Spam Box* interface with the following options:

- Enable the *Spam Box is enabled*. toggle in this interface to activate Spam Box if you did not do so in the *Spam Filters* interface.
- Click *Empty the Spam Box folder for "username"* to delete all messages in the Spam Box for the default account, where *username* represents the default account's name.
- Click *Empty all Spam Box folders* to delete all messages in the Spam Box folder for **every** email address on this account, including the default account.

### Important:

This option deletes the Spam Box folder contents for **all** email addresses on the account.

- Click *Manage Disk Usage* to select which messages you want to remove. The system directs you to the *Email Disk Usage* interface (*cPanel >> Home >> Email >> Email Disk Usage*).

## POP3 client users

If you check your email through a POP3 client, access and empty your Spam Box with the `youraddress@example.com/spam` username and your email account password. If you do not delete messages in the Spam Box frequently, spam may accumulate and cause you to reach your email account quota.

### Notes:

- You **cannot** use this method to access other folders on your account. Some webmail clients may require additional steps. For more information, read our [How to Set Up Webmail Folders](#) documentation.
- If you are unsure whether you use POP3 or IMAP to receive mail, search for this information in your email application's *Preferences* interface.

## The Spam Box feature is unavailable

For the Spam Box feature to appear, your hosting provider **must** enable the *Enable Apache SpamAssassin™ Spam Box delivery for messages marked as spam* setting in WHM's *Tweak Settings* interface (*WHM >> Home >> Server Configuration >> Tweak Settings*).

### Notes:

- If you **do not enable** the Spam Box feature but you **enable** Apache SpamAssassin, Apache SpamAssassin delivers the message to the email account's inbox as normal. However, the message's subject line will contain the phrase **\*\*\*SPAM\*\*\*** if your hosting provider enables the *Apache SpamAssassin™: X-Spam-Subject/Subject header prefix for spam emails* setting in WHM's *Exim Configuration Manager* interface (*WHM >> Home >> Service Configuration >> Exim Configuration Manager*).
- You can create filters for spam messages for all of your email accounts in cPanel's *Global Email Filters* interface (*cPanel >> Home >> Email >> Global Email Filters*), or for individual accounts in the *Email Filters* interface (*cPanel >> Home >> Email >> Email Filters*). Use email filters to direct spam if the Spam Box option does not appear in your interface.

## Automatically Delete New Spam (Auto-Delete)

Set this toggle to enabled to automatically delete messages that **meet or exceed** the Auto-Delete Threshold Score.

### Important:

Make certain that you properly configure the Auto-Delete Threshold Score. Auto-Delete permanently deletes **all** messages with a

calculated spam score that **meet or exceeds** the Auto-Delete Threshold Score. This could include **non-spam** messages, which would cause you to lose those messages.

## Configure Auto-Delete Settings

Click *Configure Auto-Delete Settings* to configure the Auto-Delete Threshold Score. The system directs you to the *Auto-Delete* interface with the following options:

- Enable the *Spam Auto-Delete is enabled*. toggle in this interface to activate Auto-Delete if you did not do so in the *Spam Filter* interface.
- Select the desired Auto-Delete Threshold Score value. Click *Update Scoring Options*. to save your changes.

**Note:**

The Auto-Delete Threshold Score does **not** affect the Spam Threshold Score.

## Additional Configurations (For Advanced Users)

This section allows you to customize the whitelist, blacklist, and individual test scores.

**Important:**

Only advanced users should configure these settings.

Click *Show Additional Configurations* to display the additional configuration options.

### Whitelist (Emails Always Allowed)

This section displays the account's current number of whitelisted items. Whitelists allow you to receive email from an email address that Apache SpamAssassin falsely marks as spam.


Click *Edit Spam Whitelist Settings* to configure the Spam Filters whitelist settings. The system directs you to the *Whitelist* interface.

**Note:**

When you add addresses to the 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 whitelist:

- `user@example.com` — Whitelists a single email address.
- `*@example.com` — Whitelists all of the addresses at `example.com`.
- `?ser@example.com` — Whitelists a single character in an address at `example.com` (for example, `user@example.com`, but not `Auser@example.com`).

To add an email address to the whitelist, perform the following steps:

1. Click *Add A New "whitelist\_from" Item* to add an email address.
2. Enter the email address in the *whitelist\_from* text box.
  - Click the cancel icon () to remove a *whitelist\_from* entry.
3. Click *Update Whitelist (whitelist\_from)* to save your changes.

### Blacklist (Emails Never Allowed)

This section displays the account's current number of blacklisted items. Blacklists allow you to mark emails that Apache SpamAssassin falsely marks as non-spam as spam mail.

Click *Edit Spam Blacklist Settings* to configure the Spam Filters blacklist settings. The system directs you to the *Blacklist* interface.


**Note:**

When you add addresses to the blacklist, 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` — Blacklist a single email address.

- `*@example.com` — Blacklist all of the addresses at `example.com`.
- `?ser@example.com` — Blacklist a single character in an address at `example.com` (for example, `user@example.com`, but not `Auser@example.com`).

To add an email address to the blacklist, perform the following steps:

1. Click *Add A New "blacklist\_from" Item* to add an email address.
2. Enter the email address in the `blacklist_from` text box.
  - Click the cancel icon () to remove a `blacklist_from` entry.
3. Click *Update Blacklist (blacklist\_from)* to save your changes.

**Note:**

To blacklist email addresses on multiple accounts, use the [Exim System Filter File](#).

## Calculated Spam Score Settings

**Warning:**

We **strongly** recommend that **only** advanced users edit the spam testing scores. Improper configurations will create unintended consequences.

Click *Configure Calculated Spam Score* to configure individual test scores. The system directs you to the *Calculated Spam Score Settings* interface.

Apache SpamAssassin uses hundreds of tests, and you can assign scores to individual tests to configure Apache SpamAssassin for your server. Use this interface to modify the individual test scores that Apache SpamAssassin uses to mark a message as spam. You can increase the score of a test that incorrectly allows spam messages to pass through. Conversely, you can disable or reduce the score of a test that falsely marks messages as spam. For example, disable tests that mark bankruptcy emails as spam for a user who is a bankruptcy lawyer.

To update an individual test score, perform the following steps:

1. Click *Add A New "scores" Item* to enter a new customized test score.
2. Select a test from the `scores` menu.
3. Enter a new value in the text box that contains up to three decimal places.

**Note:**

Set the score value to 0 to disable a test.

4. Click *Update Scoring Options* to save your changes.

**Note:**

To review default scores, run the following command at the command line:

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