


# How to Configure the Apache SpamAssassin Report\_Safe Option

Created by Unknown User (colins), last modified by Unknown User (stacy.ford) on Aug 03, 2016

- Overview
- Configure the Report\_Safe option
- Enable the Old-Style Spam System setting.
- Edit the global Apache SpamAssassin configuration file.
- Additional documentation

## Overview

The Apache SpamAssassin™ *Report\_Safe* option allows you to modify how Apache SpamAssassin alerts email recipients that an email failed its spam tests. You can configure this option in the `/etc/mail/spamassassin/local.cf` global configuration file.


 **Warnings:**

- This document is for cPanel & WHM version 11.52 and earlier. We removed the *Old-Style Spam System* setting and its functionality in cPanel & WHM version 54.
- You **must** perform **both** of the following steps to properly configure the *Report\_Safe* option.

## Configure the Report\_Safe option

1

**Enable the *Old-Style Spam System* setting.**

 **Note:**

We **removed** the *Old-Style Spam System* setting in cPanel & WHM version 54. In cPanel & WHM version 11.52 and earlier, Exim **cannot** override any changes to the `/etc/mail/spamassassin/local.cf` file when you enable this setting.

To enable this setting, perform the following steps:

- Log in to WHM as the root user.
- Navigate to WHM's [Exim Configuration Manager](#) interface (*Home >> Service Configuration >> Exim Configuration Manager*) and select the *Apache SpamAssassin™ Options* tab.
- For the *Old-Style Spam System* setting, select *On*.
- Click *Save*.

2

**Edit the global Apache SpamAssassin configuration file.**

Log in to your server via SSH as the root user and modify the `Report_Safe` value in the `/etc/mail/spamassassin/local.cf` file to use one of the following values:


Value	Description
0	Show the SPAM rules in the email header and leave the message body intact.
1	Add the following attachments: <ul style="list-style-type: none"><li>A document that details the spam rule offense.</li><li>The suspected spam email.</li></ul>
2	Cause the body of the email to include the spam rule offense text, <b>and</b> add the following attachments: <ul style="list-style-type: none"><li>A document that details the spam rule offense.</li><li>The suspected spam email.</li></ul>


## Additional documentation


- Suggested documentation


For cPanel users



For WHM users


For developers
-  [How to Configure the Apache SpamAssassin Report\\_Safe Option](#)


 [Scan Outgoing Mail](#)


 [How to Configure the Exim Outgoing IP Address](#)



 [How to Edit the exim.conf File](#)


 [CVE-2016-1531 Exim](#)
-  [How to Create a Spam Email Filter](#)


 [How to Create Mail Filter Rules For Mailing Lists](#)


 [How to Configure Mail Filters](#)

 [The BlackBerry FastMail Service](#)

 [IMAP vs. POP3](#)
-  [How to Configure the Apache SpamAssassin Report\\_Safe Option](#)

 [Scan Outgoing Mail](#)

 [How to Configure the Exim Outgoing IP Address](#)

 [How to Edit the exim.conf File](#)

 [CVE-2016-1531 Exim](#)

---

 [UAPI Functions - Chkserve::get\\_exim\\_ports\\_ssl](#)

 [WHM API 0 Functions - validate\\_exim\\_configuration\\_syntax](#)

 [UAPI Functions - Chkserve::get\\_exim\\_ports](#)

 [WHM API 0 Functions - validate\\_current\\_installed\\_exim\\_config](#)

 [WHM API 0 Functions - deliver\\_messages\\_mail\\_queue](#)

[howto](#) [spamassassin](#) [exim](#) [email](#) [whm](#)

and configuration of Internet web servers. ©2016 All rights reserved.